Kaspersky Security for Mac

Benutzerhandbuch

PROGRAMMVERSION: 13.0 CF1

Sehr geehrter Benutzer!

Vielen Dank, dass Sie unser Produkt ausgewählt haben. Wir hoffen, dass dieses Dokument Ihnen in Ihrer Arbeit hilft und die meisten aufkommenden Fragen beantwortet.

Wichtiger Hinweis: Die Rechte an diesem Dokument liegen bei der Kaspersky Lab GmbH und sind durch die Urhebergesetze der Russischen Föderation und durch internationale Abkommen geschützt. Bei illegalem Vervielfältigen und Weiterverbreiten des Dokuments oder einzelner Teile daraus kann der Beschuldigte nach geltendem Recht zivilrechtlich, verwaltungsrechtlich und strafrechtlich zur Verantwortung gezogen werden.

Das Vervielfältigen, Weiterverbreiten und Übersetzen der Unterlagen ist nur nach vorheriger schriftlicher Genehmigung von Kaspersky Lab zulässig.

Das Dokument und die dazugehörigen Grafiken dürfen nur zu informativen, nicht kommerziellen und persönlichen Zwecken verwendet werden.

Änderungen des Dokuments ohne vorherige Ankündigung bleiben vorbehalten. Die jeweils neueste Version des Dokuments finden Sie auf der Webseite von Kaspersky Lab unter der Adresse http://www.kaspersky.com/de/docs.

Für den Inhalt, die Qualität, Aktualität und Richtigkeit der im Dokument verwendeten Unterlagen, deren Rechte anderen Rechteinhabern gehören, sowie für den möglichen Schaden durch die Nutzung dieser Unterlagen, lehnt Kaspersky Lab ZAO die Haftung ab.

Erscheinungsdatum: 12.05.2012

© 2012 Kaspersky Lab ZAO. Alle Rechte vorbehalten.

www.kaspersky.de
http://support.kaspersky.com/de/

INHALT

ÜBER DIESES HANDBUCH 5
In diesem Dokument 5
Formatierung mit besonderer Bedeutung 7
INFORMATIONSQUELLEN ZUM PROGRAMM 8
Informationsquellen zur selbständigen Recherche 8
Diskussion über die Programme von Kaspersky Lab im Webforum 9
Kontaktaufnahme mit der Vertriebsabteilung 9
Kontaktaufnahme mit der Abteilung für Lokalisierung und technische Dokumentation 9
KASPERSKY SECURITY 10
Lieferumfang 11
Service für Benutzer 12
Hard- und Softwarevoraussetzungen 12
PROGRAMM INSTALLIEREN UND DEINSTALLIEREN 13
Vorbereitung der Installation des Programms 13
Vorgehen bei der Installation 13
Standardinstallation von Kaspersky Security 14
Benutzerdefinierte Installation von Kaspersky Security 15
Vorbereitung des Programmbetriebs 17
Programm deinstallieren 17
PROGRAMMOBERFLÄCHE 19
Symbol von Kaspersky Security 19
Programmhauptfenster 20
Programmkonfigurationsfenster 23
Konfigurationsfenster der Kindersicherung 24
Meldungsfenster und Pop-up-Meldungen 25
Über Meldungsfenster 26
Über Ereignistypen 26
Über Pop-up-Meldungen 26
Zustellung von Meldungen deaktivieren 26
News Agent 27
LIZENZIERUNG DES PROGRAMMS 28
Über den Lizenzvertrag 28
Über die Lizenz 28
Über den Aktivierungscode 29
Lizenz-Info anzeigen 29
Lizenz erwerben 30
Lizenz verlängern 31
Aktivierung von Kaspersky Security 32
Programm mit Testlizenz aktivieren 32
Programm mithilfe des Aktivierungscodes aktivieren 33
PROGRAMM STARTEN UND BEENDEN 34
SCHUTZSTATUS DES COMPUTERS 35
Schutzstatus des Computers einschätzen 35

Computerschutz deaktivieren 36
Computerschutz fortsetzen 37
Schutz-Center 37
LÖSUNGEN FÜR TYPISCHE AUFGABEN 39
Wie eine vollständige Virenuntersuchung des Computers ausgeführt wird 39
Computer schnell untersuchen 40
Dateien, Ordner und Laufwerke auf Viren untersuchen 40
Lizenz kaufen 40
Lizenz verlängern 41
Wie man die Datenbanken und Programm-Module aktualisiert 41
Schutz der Daten vor einem Abfangen über die Tastatur 41
Beschränken der Nutzungsdauer des Internets 42
Einschränken des Besuchs von Websites und des Downloads von Dateien aus dem Internet 43
Einschränken von Kontakten und Kommunikation des Benutzers in sozialen Netzwerken 43
Schutz persönlicher Daten vor dem Versand über soziale Netzwerke 44
Empfohlene Aktionen bei blockiertem Zugriff auf eine Datei 44
Was tun, wenn Sie vermuten, dass ein Objekt von einem Virus infiziert ist? 45
Wie ein Objekt wiederhergestellt wird, das vom Programm gelöscht oder desinfiziert wurde 46
Bericht über die Programmaktivität anzeigen 46
Empfohlene Aktionen beim Erscheinen von Meldungsfenstern und Pop-up-Meldungen 47
BEDIENUNG DES PROGRAMMS ÜBER DIE BEFEHLSZEILE 48
Hilfe anzeigen 49
Virensuche 49
Programm-Update 51
Rollback zum vorherigen Update 52
Beenden einer Komponente oder einer Aufgabe 53
Statistik über die Arbeit einer Komponente oder Aufgabe 54
Schutzparameter exportieren 54
Schutzparameter importieren 54
Programm aktivieren 55
Programm beenden 55
Rückgabecodes der Befehlszeile 55
KONTAKTAUFNAHME MIT DEM TECHNISCHEN SUPPORT 56
Wie Sie technischen Kundendienst erhalten 56
Telefonischer Technischer Support 56
Technischen Support über Mein Kaspersky Account erhalten 57
Protokolldatei verwenden 58
Protokolldatei erstellen 58
GLOSSAR 59
KASPERSKY LAB 62
INFORMATIONEN ZUM FREMDCODE 63
MARKENHINWEISE 64
SACHREGISTER 65

ÜBER DIESES HANDBUCH

Dies ist ein Benutzerhandbuch für Kaspersky Security for Mac.

Um Kaspersky Security erfolgreich verwenden zu können, sollte der Benutzer sich in der Benutzeroberfläche des Betriebssystems Mac OS X zurechtfinden sowie über Grundkenntnisse im Umgang mit der Oberfläche, Internet und dem Versand von E-Mails verfügen.

Das Handbuch dient folgenden Zwecken:

- Hilfe bei der Installation, Aktivierung und Verwendung von Kaspersky Security.
- Fragen, die sich auf Kaspersky Security beziehen, schnell beantworten.
- Hinweise auf zusätzliche Informationsquellen zum Programm und auf Möglichkeiten des technischen Supports.

IN DIESEM ABSCHNITT

In diesem Dokument 5

Formatierung mit besonderer Bedeutung 7

IN DIESEM DOKUMENT

Das Benutzerhandbuch für Kaspersky Security umfasst die folgenden Abschnitte:

Informationsquellen zum Programm (s. S. 8)

Dieser Abschnitt beschreibt Informationsquellen zum Programm und verweist auf Webseiten, die zur Diskussion über das Programm dienen.

Kaspersky Security (s. S. 10)

Dieser Abschnitt enthält eine Beschreibung der Möglichkeiten des Programms sowie eine kurze Angabe über seine Komponenten und Grundfunktionen. Hier können Sie mehr über den Lieferumfang und die Services erfahren, die den registrierten Programmnutzern zur Verfügung stehen. Außerdem werden die Hard- und Softwarevoraussetzungen genannt, denen ein Computer entsprechen muss, damit Kaspersky Security darauf installiert werden kann.

Programm installieren und deinstallieren (s. S. 13)

Dieser Abschnitt enthält Schritt-für-Schritt-Anleitungen für die Installation und Deinstallation des Programms.

Programmoberfläche (s. S. 19)

Dieser Abschnitt beschreibt die wichtigsten Elemente der grafischen Programmoberfläche: Symbol und Kontextmenü des Programms, Hauptfenster, Konfigurationsfenster, Fenster der Kindersicherung sowie Meldungsfenster.

Lizenzierung des Programms (s. S. 28)

Dieser Abschnitt informiert über die wichtigsten Begriffe, die mit der Programmaktivierung zusammenhängen. Hier werden Lizenzvertrag, Lizenztypen, Methoden zur Programmaktivierung und Verlängerung der Lizenzgültigkeit erläutert.

Programm starten und beenden (s. S. 34)

Dieser Abschnitt informiert darüber, wie das Programm gestartet und beendet wird.

Schutzstatus des Computers (s. S. 35)

Dieser Abschnitt informiert darüber, wie Bedrohungen für die Computersicherheit erkannt werden und wie die Sicherheitsstufe angepasst wird. Hier finden Sie außerdem Informationen darüber, wie der Schutz während der Arbeit des Programms aktiviert und deaktiviert werden kann.

Lösungen für typische Aufgaben (s. S. 39)

Dieser Abschnitt enthält Schritt-für-Schritt-Anleitungen für die Ausführung wichtiger Benutzeraufgaben, die vom Programm gestartet werden.

Bedienung des Programms über die Befehlszeile (s. S. 48)

In diesem Abschnitt wird ausführlich beschrieben, wie das Programm und dessen Komponenten mit der Befehlszeile bedient werden.

Kontaktaufnahme mit dem technischen Support (s. S. 56)

Dieser Abschnitt beschreibt, wie Sie technische Unterstützung erhalten, und nennt die Voraussetzungen, die dafür erfüllt sein müssen.

Glossar

Dieser Abschnitt enthält eine Liste und Definitionen von Begriffen, die in diesem Dokument vorkommen.

Kaspersky Lab" (s. S. 62)

Dieser Abschnitt enthält Informationen über ZAO Kaspersky Lab.

Informationen zum Fremdcode (s. S. 63)

Dieser Abschnitt enthält Informationen über den Code von Drittherstellern, der im Programm verwendet wird.

Markenhinweise (s. S. 64)

In diesem Abschnitt werden die Marken von Drittanbietern (Rechteinhabern) genannt, die im Dokument verwendet werden.

Sachregister

Dieser Abschnitt ermöglicht das schnelle Auffinden bestimmter Angaben in diesem Dokument.

FORMATIERUNG MIT BESONDERER BEDEUTUNG

Das Dokument enthält Textelemente (Warnungen, Tipps, Beispiele), die besondere Beachtung verdienen.

Zur Hervorhebung solcher Elemente werden spezielle Formatierungen verwendet. Ihre Bedeutung wird mit Beispielen in folgender Tabelle erläutert.

Tabelle 1. Formatierung mit besonderer Bedeutung

TEXTBEISPIEL	BESCHREIBUNG DER FORMATIERUNG
Beachten Sie bitte, dass...	Warnungen sind rot hervorgehoben und eingerahmt. Warnungen informieren darüber, dass unerwünschte Aktionen möglich sind, die zu Datenverlust oder zu Störungen des Betriebs der Geräte oder des Betriebssystems führen können.
Wir empfehlen,... zu verwenden	Hinweise sind eingerahmt. Hinweise können nützliche Tipps, Empfehlungen und spezielle Bedeutungen von Parametern enthalten oder sich auf wichtige Sonderfälle bei der Arbeit mit dem Programm beziehen.
Beispiel: ...	Beispiele sind gelb unterlegt und mit "Beispiel" überschrieben.
Das *Update* ist... Das Ereignis *Die Datenbanken sind veraltet* tritt ein.	Folgende Textelemente sind kursiv geschrieben: • neue Begriffe • Namen von Statusvarianten und Programmereignissen
Command-A	Die Tastenbezeichnungen werden durch Fettdruck hervorgehoben. Die Tastenbezeichnungen, die mit einem Minuszeichen verbunden sind, bedeuten eine Tastenkombination.
Klicken Sie auf **Aktivieren**.	Die Namen von Elementen der Programmoberfläche sind halbfett geschrieben (z.B. Eingabefelder, Menüpunkte, Schaltflächen).
➧ *Um den Zeitplan zur Ausführung des Tasks einzurichten, gehen Sie wie folgt vor:*	Der erste Satz einer Anleitung ist kursiv geschrieben und wird durch einen Pfeil markiert.
`kav update`	Folgende Textarten werden durch eine spezielle Schriftart hervorgehoben: • Text einer Befehlszeile • Text von Nachrichten, die das Programm auf dem Bildschirm anzeigt. • Daten, die vom Benutzer eingegeben werden müssen.
<IP-Adresse Ihres Computers>	Variablen stehen in eckigen Klammern. Eine Variable muss durch einen entsprechenden Wert ersetzt werden. Dabei fallen die eckigen Klammern weg.

INFORMATIONSQUELLEN ZUM PROGRAMM

Dieser Abschnitt beschreibt Informationsquellen zum Programm und verweist auf Webseiten, die zur Diskussion über das Programm dienen.

Sie können abhängig von der Dringlichkeit und Bedeutung Ihrer Frage eine passende Quelle wählen.

IN DIESEM ABSCHNITT

Informationsquellen zur selbständigen Recherche 8

Diskussion über die Programme von Kaspersky Lab im Webforum 9

Kontaktaufnahme mit der Vertriebsabteilung 9

Kontaktaufnahme mit der Abteilung für Lokalisierung und technische Dokumentation 9

INFORMATIONSQUELLEN ZUR SELBSTÄNDIGEN RECHERCHE

Sie können folgende Quellen verwenden, um nach Informationen zum Programm zu suchen:

- Webseite von Kaspersky Lab
- Webseite des technischen Supports (Wissensdatenbank)
- elektronisches Hilfesystem

Wenn Sie keine Lösung für Ihr Problem finden können, wenden Sie sich an den Technischen Support von Kaspersky Lab (s. Abschnitt "Technischer Support am Telefon" auf S. 56). Um die Informationsquellen auf der Kaspersky-Lab-Webseite zu nutzen, ist eine Internetverbindung erforderlich.

Webseite von Kaspersky Lab

Die Kaspersky-Lab-Webseite bietet für jedes Programm eine spezielle Seite.

Auf der Seite (http://www.kaspersky.com/de/kaspersky-security-for-mac) finden Sie allgemeine Informationen über das Programm, seine Funktionen und Besonderheiten.

Auf der Seite http://www.kaspersky.de befindet sich ein Link zum Internet-Shop. Dort können Sie ein Programm kaufen oder die Nutzungsrechte für das Programm verlängern.

Webseite des technischen Supports (Wissensdatenbank)

Die Wissensdatenbank auf der Webseite des Technischen Supports enthält Tipps zur Arbeit mit Kaspersky-Lab-Programmen. Die Wissensdatenbank bietet Hilfeartikel, die nach Themen angeordnet sind.

Auf der Seite des Programms finden Sie in der Wissensdatenbank (http://support.kaspersky.com/de/ksmac) nützliche Informationen, Tipps und Antworten auf häufige Fragen. Dabei werden Fragen wie Kauf, Installation und Verwendung des Programms behandelt.

Neben Fragen zu Kaspersky Security können die Artikel auch andere Kaspersky-Lab-Programme betreffen und Neuigkeiten über den Technischen Support enthalten.

Um die Wissensdatenbank aufzurufen, öffnen Sie das Programmhauptfenster (siehe Seite 20), klicken Sie auf die Schaltfläche und im folgenden Fenster auf die Schaltfläche **Technischer Support**.

Elektronisches Hilfesystem

Das elektronische Hilfesystem des Programms enthält auch eine Kontexthilfe.

Die Kontexthilfe bietet Informationen über die einzelnen Fenster und Registerkarten von Kaspersky Security (Liste und Beschreibung der Einstellungen sowie Liste der Aufgaben).

DISKUSSION ÜBER DIE PROGRAMME VON KASPERSKY LAB IM WEBFORUM

Wenn Ihre Frage keine dringende Antwort erfordert, können Sie sie mit den Spezialisten von Kaspersky Lab und mit anderen Anwendern in unserem Forum (http://forum.kaspersky.com) diskutieren.

Im Forum können Sie bereits veröffentlichte Themen nachlesen, eigene Beiträge schreiben und neue Themen eröffnen.

KONTAKTAUFNAHME MIT DER VERTRIEBSABTEILUNG

Bei Fragen zur Auswahl oder zum Kauf des Programms sowie zur Verlängerung der Nutzungsdauer stehen Ihnen die Mitarbeiter der Vertriebsabteilung zur Verfügung. Sie sind folgendermaßen zu erreichen:

- Per Kontaktformular (http://www.kasperskylab.de/kontakt/)
- Allgemeine Kontaktinformationen finden Sie unter http://www.kaspersky.com/de/impressum

Die Beratung kann auf Deutsch oder Englisch erfolgen.

KONTAKTAUFNAHME MIT DER ABTEILUNG FÜR LOKALISIERUNG UND TECHNISCHE DOKUMENTATION

Das Team für die Erstellung technischer Dokumentationen ist per E-Mail unter docfeedback@kaspersky.com zu erreichen. Geben Sie als Betreff der Nachricht "Kaspersky Help Feedback: Kaspersky Security for Mac" an.

KASPERSKY SECURITY

Kaspersky Security ermöglicht den Schutz von Computern mit dem Betriebssystem Mac OS X vor Viren und anderen Bedrohungen. Das Programm verfügt über folgende Funktionen:

Datei-Anti-Virus

Echtzeitschutz für das Dateisystem des Computers: Zugriffe auf das Dateisystem werden abgefangen und analysiert, schädliche Objekte werden desinfiziert oder gelöscht, möglicherweise infizierte Objekte werden für spätere Analyse isoliert.

Web-Anti-Virus und Anti-Phishing

Schutz von Informationen, die über das HTTP- und HTTPS-Protokoll auf Ihren Computer gelangen. Überprüfung der Website-Links auf Phishing-Links und verdächtige Webadressen mithilfe des Moduls zur Link-Untersuchung. Verhindern des Abfangens von persönlichen Daten, die über die Tastatur eingegeben werden, mithilfe der Virtuellen Tastatur.

Virensuche

Manuelle Suche und Neutralisierung von Viren und anderen Bedrohungen auf Anfrage des Benutzers: In festgelegten Untersuchungsbereichen werden infizierte und möglicherweise infizierte Objekte gesucht und analysiert, Objekte werden desinfiziert, gelöscht oder für spätere Analyse isoliert.

In Kaspersky Security sind folgende Untersuchungsaufgaben enthalten: vollständige Untersuchung aller Objekte des Computers und schnelle Untersuchung von kritischen Bereichen.

Update

Aktualisierung der Anti-Viren-Datenbanken und Module, die zum Lieferumfang von Kaspersky Security gehören, über den Kaspersky-Lab-Updateserver; Erstellung von Sicherungskopien aller zu aktualisierenden Dateien, um das letzte Update bei Bedarf rückgängig zu machen (Rollback).

Kindersicherung

Kontrolle über die Aktionen verschiedener Benutzer am Computer und im Internet: Der Internetzugang sowie der Zugriff auf Webressourcen und Programme werden zeitlich beschränkt, Listen mit Kontakten werden erstellt, für die die Kommunikation in sozialen Netzwerken erlaubt oder verboten ist, der Versand bestimmter persönlicher Daten wird verboten, es können Berichte über die Aktionen der Benutzer angezeigt werden.

Quarantäne

Verschieben von möglicherweise infizierten Objekten in die Quarantäne: Möglicherweise infizierte Objekte werden in einem Quarantäneordner gespeichert. Sie können später mit aktualisierten Datenbanken untersucht oder vom Benutzer manuell aus der Quarantäne wiederhergestellt werden.

Backup

Vor dem Desinfizieren oder Löschen eines Objekts wird im Backup eine Sicherungskopie davon angelegt. Dadurch besteht die Möglichkeit, das Objekt wiederherzustellen, um darin enthaltene Informationen zu retten.

Berichte

Erstellen eines ausführlichen Berichts über die Arbeit der einzelnen Komponenten von Kaspersky Security.

Benachrichtigungen

Der Benutzer wird über das Eintreten von Ereignissen bei der Ausführung von Kaspersky Security mithilfe von Meldungsfenstern und Pop-up-Meldungen informiert, die mit Signaltönen ergänzt werden können.

Bei der Arbeit mit Kaspersky Security werden Sie umfassend mit Informationen unterstützt: die Anwendung zeigt Meldungen über den Schutzstatus an und verfügt über ein umfassendes Hilfesystem. Der im Schutz-Center enthaltene Sicherheitsassistent (auf Seite 37) vermittelt Ihnen ein vollständiges Bild des aktuellen Schutzzustands Ihres Computers und ermöglicht die umgehende Behebung vorhandener Probleme.

IN DIESEM ABSCHNITT

Lieferumfang 11

Service für Benutzer 12

Hard- und Softwarevoraussetzungen 12

LIEFERUMFANG

Sie können das Programm folgendermaßen kaufen:

- **In einer Box**. Verkauf über unsere Vertriebspartner.
- **Über einen Internet-Shop**. Verkauf über einen Internet-Shop von Kaspersky Lab (beispielsweise http://www.kaspersky.de, Link **Online-Shop**) oder unserer Vertriebspartner.

Wenn Sie das Programm in einer CD-Box erworben haben, umfasst der Lieferumfang folgende Elemente:

- versiegelter Umschlag mit Installations-CD, auf der die Programmdateien und die Dateien der Programmdokumentation gespeichert sind.
- Kurzes Benutzerhandbuch, das einen Aktivierungscode für das Programm enthält.
- Lizenzvertrag, der die Nutzungsbedingungen für das Programm festlegt.

Der Lieferumfang kann sich je nach Region, in der das Programm vertrieben wird, unterscheiden.

Wenn Sie Kaspersky Security in einem Internet-Shop kaufen, kopieren Sie das Programm von der Webseite des Internet-Shops. Sie erhalten die Programmaktivierung erforderlichen Informationen nach Eingang des Rechnungsbetrags per E-Mail.

Ausführliche Informationen zum Kauf und Lieferumfang erhalten Sie bei unserer Vertriebsabteilung (sales@kaspersky.com).

SERVICE FÜR BENUTZER

Wenn Sie eine Lizenz für die Nutzung des Programms erwerben, können Sie im Laufe der Gültigkeitsdauer der Lizenz folgende Dienste in Anspruch nehmen:

- Update der Datenbanken und Nutzung neuer Programmversionen
- Beratung bei Fragen zur Installation, Konfiguration und Nutzung des Programms per Telefon und E-Mail
- Benachrichtigung über die Veröffentlichung neuer Programme von Kaspersky Lab sowie Informationen über neue Viren und Virenepidemien. Diesen Service können Sie nutzen, wenn Sie auf der Webseite des Technischen Supports den Newsletter von Kaspersky Lab abonnieren.

Die Beratung erstreckt sich nicht auf Fragen über die Funktionsweise von Betriebssystemen, der Software von Drittherstellern und sonstiger Technologien.

HARD- UND SOFTWAREVORAUSSETZUNGEN

Um die normale Funktionsfähigkeit von Kaspersky Security zu gewährleisten, sind folgende Systemvoraussetzungen zu erfüllen:

- Betriebssystem Mac OS X 10.6, 10.7 oder 10.8;
- 350 MB freier Festplattenspeicher (je nach Größe der Antiviren-Datenbanken).

PROGRAMM INSTALLIEREN UND DEINSTALLIEREN

Dieser Abschnitt enthält Schritt-für-Schritt-Anleitungen für die Installation und Deinstallation des Programms.

Zum Lieferumfang von Kaspersky Security gehört das Installations- und Deinstallationsprogramm für Kaspersky Security.

IN DIESEM ABSCHNITT

Vorbereitung der Installation des Programms 13

Vorgehen bei der Installation 13

Vorbereitung des Programmbetriebs 17

Programm deinstallieren 17

VORBEREITUNG DER INSTALLATION DES PROGRAMMS

Vor der Installation von Kaspersky Security sollten Sie die folgenden Vorbereitungen treffen:

- Vergewissern Sie sich, dass Ihr Computer die Hard- und Softwarevoraussetzungen (s. Abschnitt "Hard- und Softwarevoraussetzungen" auf Seite 12) erfüllt.
- Überprüfen Sie die Verbindung Ihres Computers mit dem Internet. Zugriff auf das Internet ist für die Aktivierung des Programms mithilfe eines Aktivierungscodes sowie zum Download von Updates erforderlich.
- Deinstallieren Sie sonstige Antiviren-Software von Ihrem Computer, um Systemkonflikte und eine Verringerung der Arbeitsgeschwindigkeit des Betriebssystems zu vermeiden.

VORGEHEN BEI DER INSTALLATION

Sie können eine der folgenden Methoden zur Installation von Kaspersky Security auf Ihrem Computer auswählen:

- Standardinstallation.

  Ermöglicht es, die Standard-Programmkomponenten zu installieren.

- Benutzerdefinierte Installation.

  Ermöglicht es, Programmkomponenten manuell zu installieren. Die manuelle Installation wird nur erfahrenen Computernutzern empfohlen.

IN DIESEM ABSCHNITT

Standardinstallation von Kaspersky Security 14

Benutzerdefinierte Installation von Kaspersky Security 15

STANDARDINSTALLATION VON KASPERSKY SECURITY

Gehen Sie folgendermaßen vor, um die Standardinstallation von Kaspersky Security auszuführen:

1. Öffnen Sie die mitgelieferten Dateien von Kaspersky Security. Legen sie dafür die Installations-CD ins Laufwerk.

   Wenn Sie Kaspersky Security in einem Internet-Shop gekauft haben, können Sie auf der Website von Kaspersky Lab ein Programmpaket im dmg-Format herunterladen. Starten Sie die dmg-Datei, um den Inhalt des Programmpakets anzusehen.

2. Starten Sie das Installationsprogramm von Kaspersky Security. Gehen Sie dazu folgendermaßen vor:

   a. Öffnen Sie im Fenster mit dem Distributionsinhalt das Installationspaket **Kaspersky Security**.

   b. Bestätigen Sie den Start des Installationsprogramms im Bestätigungsfenster. Klicken Sie dazu im Abfragefenster auf **Fortfahren**.

      Befolgen Sie die Schritte des Installationsprogramms, um das Programm zu installieren.

3. Lesen Sie im Fenster **Einführung** die Informationen über das zu installierende Programm durch und stellen Sie sicher, dass Ihr Computer die angegebenen Hardware- und Software-Anforderungen erfüllt.

   Klicken Sie auf die Schaltfläche **Fortfahren**, um mit der Installation fortzufahren.

4. Machen Sie sich im Fenster **Lizenz** mit der Lizenzvereinbarung zur Nutzung von Kaspersky Security vertraut, die zwischen Ihnen und Kaspersky Lab ZAO abgeschlossen wird. Sie können folgende Aktionen ausführen:

   - Text des Lizenzvertrags drucken. Klicken Sie dazu auf die Schaltfläche **Drucken**.
   - Lizenzvertrag als Textdatei speichern. Klicken Sie dazu auf die Schaltfläche **Sichern**.
   - Programminstallation fortsetzen. Klicken Sie dazu auf die Schaltfläche **Fortfahren**.

     Daraufhin erscheint das Bestätigungsfenster für Ihre Zustimmung zu den Bedingungen der Lizenzvereinbarung. Führen Sie eine der folgenden Aktionen aus:

     - Mit der Installation von Kaspersky Security fortfahren, wenn Sie mit allen Punkten des Lizenzvertrags einverstanden sind. Klicken Sie dazu auf die Schaltfläche **Akzeptieren**.
     - Zur Lizenzvereinbarung zurückkehren. Klicken Sie dazu auf die Schaltfläche **Lizenz lesen**.
     - Programminstallation abbrechen, wenn Sie mit dem Lizenzvertrag nicht einverstanden sind. Klicken Sie dazu auf die Schaltfläche **Ablehnen**.

5. Lesen Sie im Fenster **KSN** die Informationen zur Teilnahme am Kaspersky Security Network durch. Die Teilnahme am Kaspersky Security Network sieht vor, dass Informationen über auf Ihrem Computer erkannte neue Bedrohungen, über gestartete Programme und über geladene signierte Programme an Kaspersky Lab geschickt werden. Außerdem werden ein einmaliger Identifikator, der Ihrem Exemplar von Kaspersky Security zugewiesen wurde, sowie Systeminformationen gesendet. Es wird garantiert, dass keine persönlichen Daten gesendet werden.

   Wenn Sie mit allen Punkten der Bestimmung über die Verwendung von Kaspersky Security Network einverstanden sind, aktivieren Sie das Kontrollkästchen **Ich akzeptiere die Teilnahmebedingungen an KSN**.

   Klicken Sie auf die Schaltfläche **Fortfahren**, um mit der Installation fortzufahren.

   Sie können jederzeit Ihre Teilnahme an Kaspersky Security Network verweigern.

6. Lesen Sie im Fenster **Installationstyp** sorgfältig alle Informationen zum Volume durch, auf dem das Programm installiert werden soll, und informieren Sie sich über den für die Installation benötigten freien Speicherplatz auf dem Datenträger.

   Wenn Sie einen anderen Datenträger für die Programminstallation wählen möchten, klicken Sie auf die Schaltfläche **Ort für die Installation ändern** und wählen Sie im Fenster **Zielvolume auswählen** ein anderes Volume. Klicken Sie auf die Schaltfläche **Fortfahren**.

   Um das Programm mit den vorgeschlagenen Standardeinstellungen zu installieren, klicken Sie auf die Schaltfläche **Installieren**. Bestätigen Sie die Programminstallation im Abfragefenster.

   Das Laufwerk für die Installation des Programms muss ein Boot-Laufwerk sein. Das Betriebssystem auf diesem Laufwerk darf nicht älter als die in den Hard- und Softwarevoraussetzungen angegebene Version sein (s. Abschnitt "Hard- und Softwarevoraussetzungen" auf Seite 12).

7. Warten Sie, bis das Installationsprogramm für Kaspersky Security die Programmkomponenten installiert hat.

8. Lesen Sie Informationen zum Abschluss des Installationsvorgangs im Fenster **Zusammenfassung** durch, und klicken Sie auf die Schaltfläche **Schließen**, um das Installationsprogramm zu beenden.

Nach Fertigstellung der Installation wird Kaspersky Security automatisch gestartet. Ein Neustart des Computers ist nicht erforderlich.

BENUTZERDEFINIERTE INSTALLATION VON KASPERSKY SECURITY

Gehen Sie folgendermaßen vor, um die benutzerdefinierte Installation von Kaspersky Security auszuführen:

1. Öffnen Sie die mitgelieferten Dateien von Kaspersky Security. Legen sie dafür die Installations-CD ins Laufwerk.

   Wenn Sie Kaspersky Security in einem Internet-Shop gekauft haben, können Sie auf der Website von Kaspersky Lab ein Programmpaket im dmg-Format herunterladen. Starten Sie die dmg-Datei, um den Inhalt des Programmpakets anzusehen.

2. Starten Sie das Installationsprogramm von Kaspersky Security. Gehen Sie dazu folgendermaßen vor:

   a. Öffnen Sie im Fenster mit dem Distributionsinhalt das Installationspaket **Kaspersky Security**.

   b. Bestätigen Sie den Start des Installationsprogramms im Bestätigungsfenster. Klicken Sie dazu im Abfragefenster auf **Fortfahren**.

      Befolgen Sie die Schritte des Installationsprogramms, um das Programm zu installieren.

3. Lesen Sie im Fenster **Einführung** die Informationen über das zu installierende Programm durch und stellen Sie sicher, dass Ihr Computer die angegebenen Hardware- und Software-Anforderungen erfüllt.

   Klicken Sie auf die Schaltfläche **Fortfahren**, um mit der Installation fortzufahren.

4. Machen Sie sich im Fenster **Lizenz** mit der Lizenzvereinbarung zur Nutzung von Kaspersky Security vertraut, die zwischen Ihnen und Kaspersky Lab ZAO abgeschlossen wird. Sie können folgende Aktionen ausführen:

   - Text des Lizenzvertrags drucken. Klicken Sie dazu auf die Schaltfläche **Drucken**.
   - Lizenzvertrag als Textdatei speichern. Klicken Sie dazu auf die Schaltfläche **Sichern**.
   - Programminstallation fortsetzen. Klicken Sie dazu auf die Schaltfläche **Fortfahren**.

     Daraufhin erscheint das Bestätigungsfenster für Ihre Zustimmung zu den Bedingungen der Lizenzvereinbarung. Führen Sie eine der folgenden Aktionen aus:

- Mit der Installation von Kaspersky Security fortfahren, wenn Sie mit allen Punkten des Lizenzvertrags einverstanden sind. Klicken Sie dazu auf die Schaltfläche **Akzeptieren**.
- Zur Lizenzvereinbarung zurückkehren. Klicken Sie dazu auf die Schaltfläche **Lizenz lesen**.
- Programminstallation abbrechen, wenn Sie mit dem Lizenzvertrag nicht einverstanden sind. Klicken Sie dazu auf die Schaltfläche **Ablehnen**.

5. Lesen Sie im Fenster **KSN** die Informationen zur Teilnahme am Kaspersky Security Network durch. Die Teilnahme am Kaspersky Security Network sieht vor, dass Informationen über auf Ihrem Computer erkannte neue Bedrohungen, über gestartete Programme und über geladene signierte Programme an Kaspersky Lab geschickt werden. Außerdem werden ein einmaliger Identifikator, der Ihrem Exemplar von Kaspersky Security zugewiesen wurde, sowie Systeminformationen gesendet. Es wird garantiert, dass keine persönlichen Daten gesendet werden.

   Wenn Sie mit allen Punkten der Bestimmung über die Verwendung von Kaspersky Security Network einverstanden sind, aktivieren Sie das Kontrollkästchen **Ich akzeptiere die Teilnahmebedingungen an KSN**.

   Klicken Sie auf die Schaltfläche **Fortfahren**, um mit der Installation fortzufahren.

   Sie können jederzeit Ihre Teilnahme an Kaspersky Security Network verweigern.

6. Lesen Sie im Fenster **Installationstyp** sorgfältig alle Informationen zum Volume durch, auf dem das Programm installiert werden soll, und informieren Sie sich über den für die Installation benötigten freien Speicherplatz auf dem Datenträger.

   Wenn Sie einen anderen Datenträger für die Programminstallation wählen möchten, klicken Sie auf die Schaltfläche **Ort für die Installation ändern** und wählen Sie im Fenster **Zielvolume auswählen** ein anderes Volume. Klicken Sie auf die Schaltfläche **Fortfahren**.

   Das Laufwerk für die Installation des Programms muss ein Boot-Laufwerk sein. Das Betriebssystem auf diesem Laufwerk darf nicht älter als die in den Systemvoraussetzungen angegebene Version sein (s. Abschnitt "Hard- und Softwarevoraussetzungen" auf Seite 12).

   Um Programmkomponenten für eine benutzerdefinierte Installation auszuwählen, klicken Sie auf die Schaltfläche **Einstellungen**.

7. Geben Sie im folgenden Fenster an, welche Programmkomponenten auf dem Computer installiert werden sollen. Deaktivieren Sie die Kontrollkästchen neben den Namen der Komponenten, die nicht installiert werden sollen. Standardmäßig sind alle Kontrollkästchen aktiviert, sodass alle Programmkomponenten auf dem Computer installiert werden.

   - **Virensuche**. Diese Komponente ermöglicht eine Untersuchung von Objekten in benutzerdefinierten Bereichen.

     Diese Komponente von Kaspersky Security wird immer installiert.

   - **Datei-Anti-Virus**. Diese Komponente untersucht in Echtzeit alle Dateien, die vom Benutzer geöffnet, gestartet und gespeichert werden.
   - **Web-Anti-Virus**. Diese Komponente verhindert das Eindringen von Viren und anderen Bedrohungen über das HTTP- und HTTPS-Protokoll.
   - **Kindersicherung**. Diese Komponente bietet Kontrolle über die Aktionen verschiedener Benutzer auf einem Computer und im Internet.
   - **Modul zur Link-Untersuchung**. Diese Komponente ermöglicht die Untersuchung von Links in Browsern auf ihre Sicherheit.

- **Virtuelle Tastatur**. Diese Komponente ermöglicht eine sichere Eingabe von Kennwörtern und sonstigen Geheiminformationen.

Klicken Sie nach der Auswahl der Komponenten auf **Installieren**. Bestätigen Sie die Programminstallation im Abfragefenster.

Wenn Sie zu den Standardeinstellungen der Installation zurückkehren möchten, klicken Sie auf **Standardinstallation**.

8. Warten Sie, bis das Installationsprogramm Kaspersky Security die ausgewählten Programmkomponenten installiert hat.

9. Lesen Sie Informationen zum Abschluss des Installationsvorgangs im Fenster **Durchsuchen** durch, und klicken Sie auf die Schaltfläche **Schließen**, um das Installationsprogramm zu beenden.

Nach Fertigstellung der Installation wird Kaspersky Security automatisch gestartet. Ein Neustart des Computers ist nicht erforderlich.

VORBEREITUNG DES PROGRAMMBETRIEBS

Nach der Installation von Kaspersky Security sollten Sie folgende Aktionen ausführen:

- Kaspersky Security aktivieren (s. Abschnitt "Kaspersky Security aktivieren" auf Seite 32). Die Verwendung des Programms unter der kommerziellen Lizenz ermöglicht Ihnen, Ihre Antiviren-Datenbanken und Programm-Module regelmäßig zu aktualisieren, und gewährt Ihnen Zugriff auf den Technischen Support.

- Aktuellen Schutzzustand einschätzen (siehe Abschnitt "Schutzstatus des Computers einschätzen" auf Seite 35), um sicherzustellen, dass Kaspersky Security den Schutz auf der erforderlichen Stufe gewährleistet.

- Kaspersky Security aktualisieren (siehe Abschnitt "Wie man die Datenbanken und Programm-Module aktualisiert" auf Seite 41). Die Antiviren-Datenbanken und Module von Kaspersky Security müssen stets auf dem neuesten Stand sein, damit das Programm jederzeit Viren und andere Bedrohungen finden und desinfizieren kann.

- Vollständige Untersuchung des Computers auf Viren und andere Bedrohungen ausführen (siehe Abschnitt "Computer vollständig auf Viren untersuchen" auf Seite 39).

Falls während des Programmbetriebs Probleme oder Fehler auftreten, sollten Sie das Fenster mit Berichten über die Ausführung von Kaspersky Security öffnen (s. Abschnitt "Bericht über die Programmaktivität anzeigen" auf Seite 46). Möglicherweise können Sie den Grund der Störung dem Bericht entnehmen. Wenn es Ihnen nicht gelingt, das Problem selbst zu lösen, wenden Sie sich an den Technischen Support von Kaspersky Lab (siehe Abschnitt "Kontaktaufnahme mit dem Technischen Support" auf Seite 56).

PROGRAMM DEINSTALLIEREN

Nach der Deinstallation von Kaspersky Security besteht ein ernsthaftes Infektionsrisiko für Ihren Computer.

Es wird empfohlen, vor der Deinstallation des Programms alle Objekte zu bearbeiten, die in der Quarantäne und im Backup gespeichert sind. Alle unbearbeiteten Quarantäne- und Backup-Objekte werden unwiderruflich gelöscht.

➧ *Gehen Sie folgendermaßen vor, um Kaspersky Security zu deinstallieren:*

1. Öffnen Sie die mitgelieferten Dateien von Kaspersky Security. Legen sie dafür die Installations-CD ins Laufwerk.

Wenn Sie Kaspersky Security in einem Internet-Shop gekauft haben, können Sie auf der Website von Kaspersky Lab ein Programmpaket im dmg-Format herunterladen. Starten Sie die dmg-Datei, um den Inhalt des Programmpakets anzusehen.

2. Starten Sie das Deinstallationsprogramm von Kaspersky Security. Wählen Sie dazu im Fenster mit den mitgelieferten Dateien **Kaspersky Security deinstallieren** aus.

   Befolgen Sie die Schritte des Deinstallationsprogramms, um Kaspersky Security zu deinstallieren.

3. Klicken Sie im Fenster **Einführung** auf die Schaltfläche **Löschen**. Bestätigen Sie die Deinstallation des Programms im Abfragefenster.

4. Warten Sie, bis das Deinstallationsprogramm Kaspersky Security vom Computer deinstalliert hat.

5. Lesen Sie Informationen zum Abschluss des Deinstallationsvorgangs im Fenster **Ende** durch, und klicken Sie auf die Schaltfläche **Fertig**, um das Deinstallationsprogramm zu beenden.

Ein Neustart des Computers ist nach der Deinstallation von Kaspersky Security nicht erforderlich.

PROGRAMMOBERFLÄCHE

Dieser Abschnitt beschreibt die wichtigsten Elemente der grafischen Programmoberfläche: Symbol und Kontextmenü des Programms, Hauptfenster, Konfigurationsfenster, Fenster der Kindersicherung sowie Meldungsfenster.

IN DIESEM ABSCHNITT

Symbol von Kaspersky Security 19

Programmhauptfenster 20

Programmkonfigurationsfenster 23

Konfigurationsfenster der Kindersicherung 24

Meldungsfenster und Pop-up-Meldungen 25

News Agent 27

SYMBOL VON KASPERSKY SECURITY

Sofort nach der Installation von Kaspersky Security erscheint in der Menüleiste das Programmsymbol. Das Symbol dient als Indikator für die Programmfunktionen. Wenn das Programmsymbol aktiv ist, ist der Echtzeitschutz des Computers vor schädlichen Programmen aktiviert. Das inaktive Programmsymbol deutet darauf hin, dass der Schutz ausgeschaltet ist.

Das Symbol von Kaspersky Security befindet sich standardmäßig in der Menüleiste. In der Dock-Schnellstartleiste erscheint das Programmsymbol von Kaspersky Security nur dann, wenn eines der Programmfenster geöffnet ist.

Das Kontextmenü bietet Zugriff (siehe Abbildung unten) auf die wichtigsten Befehle für Kaspersky Security:

- Computerschutz deaktivieren
- Computerschutz fortsetzen
- Schutz-Center öffnen
- Updateaufgabe starten
- Schnelle Virenuntersuchung des Computers starten
- Konfigurationsfenster der Kindersicherung öffnen
- Programmkonfigurationsfenster öffnen

Um das Kontextmenü des Symbols von Kaspersky Security,

klicken Sie in der Menüleiste auf das Programmsymbol.

Abbildung 1. Kontextmenü des Symbols von Kaspersky Security in der Menüleiste

PROGRAMMHAUPTFENSTER

Gehen Sie folgendermaßen vor, um das Programmhauptfenster zu öffnen:

1. Klicken Sie in der Menüleiste auf das Symbol von Kaspersky Security.
2. Wählen Sie im Kontextmenü des Programmsymbols den Punkt **Kaspersky Security**.

Aufgaben des Programmhauptfensters

Die wichtigsten Aufgaben des Hauptfensters von Kaspersky Security (siehe Abbildung unten) bestehen darin, den Benutzer über den Zustand des Computerschutzes und über vorhandene Probleme zu informieren, und Informationen über die Arbeit Datei-Anti-Virus, Web-Anti-Virus sowie über die Ausführung der Untersuchungsaufgaben und der Updateaufgabe zu bieten.

Vom Programmhauptfenster aus können Sie außerdem:

- Programm-Update starten
- Untersuchungsaufgaben starten
- Zur Lizenzverwaltung des Programms wechseln
- Fenster des Schutz-Centers öffnen

- Programmkonfigurationsfenster öffnen
- Berichtsfenster öffnen
- News Agent öffnen

Abbildung 2. Hauptfenster von Kaspersky Security

Steuerelemente im Programmhauptfenster

Es gibt drei Varianten für den Schutzstatus des Computers (s. Abschnitt "Schutzstatus des Computers einschätzen" auf Seite 35).

Der aktuelle Schutzstatus wird durch die Farbe des Statusindikators für den Computerschutz signalisiert.

- Grün bedeutet, dass der Schutz Ihres Computers dem erforderlichen Niveau entspricht.
- Gelb und Rot signalisieren, dass in den Einstellungen oder bei der Arbeit von Kaspersky Security Probleme vorliegen.

Um ausführliche Informationen über diese Probleme zu erhalten und sie zu beheben, können Sie das Schutz-Center verwenden (s. Abschnitt "Schutz-Center" auf Seite 37). Das Fenster des Schutz-Centers wird durch einen Klick auf den Statusindikator für den Computerschutz geöffnet.

Im linken Bereich des Programmhauptfensters wird der Statusindikator für den Computerschutz durch Textinformationen über den Schutzstatus des Computers ergänzt und es werden Sicherheitsrisiken genannt, falls das Schutz-Center solche erkannt hat. Außerdem werden im linken Bereich des Programmhauptfensters Informationen über die Ausführung laufender Untersuchungsaufgaben oder der Updateaufgabe (mit Prozentangabe) angezeigt.

Mit den Schaltflächen im Programmhauptfenster können Sie folgende Aktionen ausführen:

Update von Kaspersky Security starten. Nach Abschluss des Updates werden im Berichtsfenster Detailinformationen über die abgeschlossene Updateaufgabe angezeigt.

Zu den Untersuchungsaufgaben Schnelle Suche, Vollständige Suche und Virensuche in dem durch den Benutzer vorgegebenen Bereich wechseln. Nach Abschluss der Virensuche werden im Berichtsfenster Detailinformationen über die abgeschlossene Aufgabe angezeigt.

Zu dem Fenster wechseln, das Informationen zur verwendeten Lizenz enthält (s. Abschnitt "Lizenz-Info anzeigen" auf Seite 29), und auf die Lizenzverwaltung des Programms zugreifen.

Im oberen Bereich des Programmhauptfensters befindet sich eine Navigationsleiste. Mit den Schaltflächen in der Navigationsleiste können Sie folgende Aktionen ausführen:

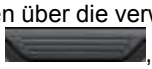
Das Berichtsfenster für Kaspersky Security öffnen, auf die Quarantäne und den Backupordner zugreifen.

Das Programmkonfigurationsfenster öffnen (siehe Seite 23).

Die elektronische Hilfe für Kaspersky Security öffnen.

Ein Fenster mit Informationen über die Möglichkeiten, den technischen Support in Anspruch zu nehmen, öffnen(siehe Abschnitt "Kontaktaufnahme mit dem technischen Support" auf Seite 56).

Fenster von News Agent mit einer Nachrichtenliste öffnen (s. Abschnitt "News Agent" auf Seite 27). Diese Schaltfläche wird angezeigt, nachdem Kaspersky Security Nachrichten empfangen hat.

Im unteren Bereich des Hauptfensters befindet sich die Schaltfläche . Klicken Sie auf die Schaltfläche, um die Symbolleiste zu erweitern, die eine zusammenfassende Statistik über die Arbeit von Datei-Anti-Virus sowie Informationen über die verwendeten Antiviren-Datenbanken des Programms enthält. Klicken Sie erneut auf die Schaltfläche  , um die Symbolleiste zu minimieren.

Außerdem befinden sich im unteren Bereich des Programmhauptfensters Indikatoren für Datei-Anti-Virus, Web-Anti-Virus und die Kindersicherung. Die grüne Farbe des Indikators bedeutet, dass die Komponente ausgeführt wird, Rot signalisiert eine Störung der Komponente. Der graue Indikator bedeutet, dass die Komponente deaktiviert oder nicht installiert wurde.

Mit den Schaltflächen, die sich neben den Indikatoren für Datei-Anti-Virus, Web-Anti-Virus und die Kindersicherung befinden, gelangen Sie zu den Einstellungen für die Komponenten.

PROGRAMMKONFIGURATIONSFENSTER

Das Konfigurationsfenster für Kaspersky Security (siehe Abbildung unten) können Sie auf folgende Weise öffnen:

- durch Klicken auf die Schaltfläche im Programmhauptfenster (siehe Abschnitt "Programmhauptfenster" auf Seite 20);
- Auswahl des Punktes **Einstellungen** im Kontextmenü des Symbols von Kaspersky Security (s. Abschnitt "Symbol von " auf Seite 19).

Abbildung 3. Programmkonfigurationsfenster. Registerkarte Schutz

Im oberen Bereich des Programmkonfigurationsfensters befinden sich Registerkarten. Die Registerkarten dienen dem Zugriff auf folgende Programmfunktionen:

- Anpassen von Datei-Anti-Virus und Web-Anti-Virus auf der Registerkarte **Schutz**;
- Anpassen der Untersuchungsaufgaben auf der Registerkarte **Virensuche**;

- Anpassen der Teilnahme am Kaspersky Security Network auf der Registerkarte **KSN**;
- Auswahl der zu kontrollierenden schädlichen Programme und Anlegen der vertrauenswürdigen Zone auf der Registerkarte **Bedrohungen**;
- Anpassen des Programm-Updates auf der Registerkarte **Update**;
- Anpassen der Einstellungen für Berichte und Speicher für Kaspersky Security auf der Registerkarte **Berichte**;
- Service-Einstellungen für Kaspersky Security auf der Registerkarte **Ansicht**.

Die Feineinstellung bestimmter Parameter erfolgt in Konfigurationsfenstern der zweiten und dritten Ebene.

Sie können die Veränderung der Einstellungen von Kaspersky Security für Benutzer, die keine Administratorrechte besitzen, mithilfe der Schaltfläche sperren. Die Schaltfläche befindet sich im unteren Bereich des Konfigurationsfensters. Um diese Sperre wieder aufzuheben, geben Sie die Benutzerdaten des Computeradministrators ein.

Die Schaltfläche bietet Zugriff auf das Hilfesystem von Kaspersky Security mit einer Beschreibung der Parameter für das aktuelle Anwendungsfenster. Sie können auch auf die Hilfe für das aktuelle Programmfenster zugreifen, indem Sie im Menü **Hilfe** den Punkt **Hilfe für dieses Fenster öffnen** auswählen.

KONFIGURATIONSFENSTER DER KINDERSICHERUNG

Sie können das Konfigurationsfenster für die Kindersicherung wie folgt aufrufen:

- Auswahl des Punktes **Kindersicherung** im Kontextmenü des Symbols von Kaspersky Security (s. Abschnitt "Symbols von Kaspersky Security" auf Seite 19);
- Über die Schaltfläche, die sich neben dem Indikator für die Kindersicherung im unteren Bereich des Programmhauptfensters befindet (s. Abschnitt "Programmhauptfenster" auf Seite 20).

Im linken Bereich des Konfigurationsfensters für die Kindersicherung (siehe Abbildung unten) befindet sich eine Liste mit den Benutzerkonten der Computerbenutzer. Neben dem Namen des Benutzerkontos befindet sich der Indikator für die Kindersicherung für dieses Benutzerkonto. Der Indikator ist grün, wenn die Kindersicherung aktiviert ist. Rot signalisiert, dass die Kindersicherung deaktiviert wurde. Standardmäßig ist die Kindersicherung für alle Benutzerkonten deaktiviert. Sie können die Kindersicherung aktivieren.

Wenn die Kindersicherung für das Benutzerkonto aktiviert ist, können Sie im rechten Bereich des Konfigurationsfensters für die Kindersicherung auf der Registerkarte **Einstellungen** (siehe Abbildung unten) auswählen, welche Aktionen dieses Benutzers auf dem Computer und im Internet kontrolliert werden sollen.

Kaspersky Security kontrolliert folgende Benutzeraktionen nach folgenden Kategorien:

- **Web-Kontrolle** – Kontrolle über Websites und den Download von Dateien.
- **Zeitkontrolle** – Zeitkontrolle des Internetzugangs.

- **Persönliche Daten** – Kontrolle über die Nutzung persönlicher Daten.
- **Soziale Netzwerke** – Kontrolle über die Nutzung sozialer Netzwerke.

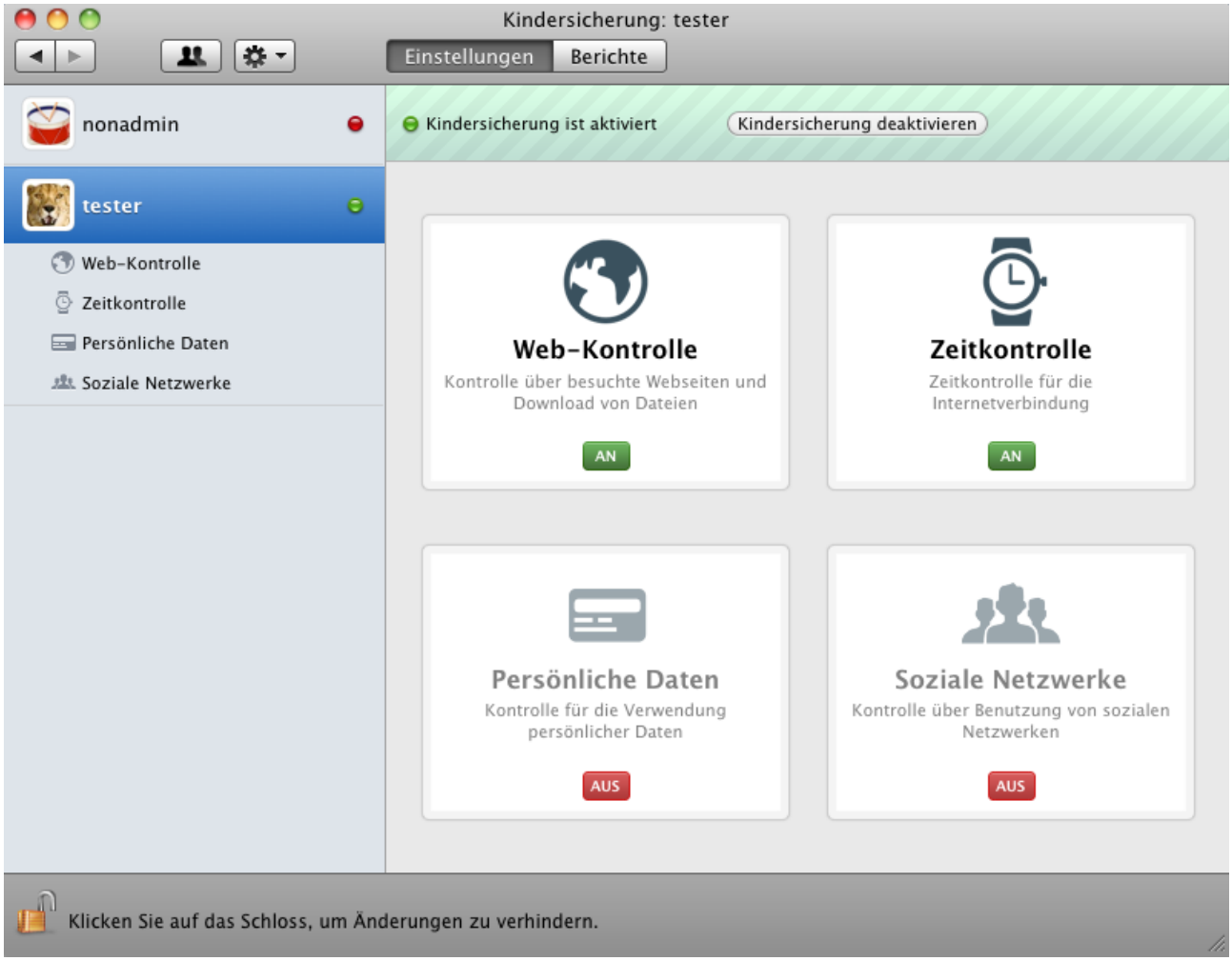


Abbildung 4. Konfigurationsfenster der Kindersicherung. Registerkarte Einstellungen

Standardmäßig ist die Kontrolle der Benutzeraktionen für alle Kategorien deaktiviert. Sie können die Kontrolle für jede Kategorie der Benutzeraktionen einzeln aktivieren und zur ausführlichen Anpassung der ausgewählten Kategorie im rechten Bereich des Konfigurationsfensters für die Kindersicherung wechseln.

Darüber hinaus können Sie für das Benutzerkonto, für das die Kindersicherung aktiviert ist, separat für jede Kategorie Berichte über die Aktionen eines Benutzers anzeigen lassen. Wählen Sie dazu die Registerkarte **Berichte** im rechten Bereich des Konfigurationsfensters für die Kindersicherung.

Für Benutzer, die keine Administratorrechte besitzen, ist die Anpassung der Kindersicherung gesperrt. Klicken Sie auf die Schaltfläche und geben Sie die Benutzerdaten des Computeradministrators an, um die Berichte zur Kindersicherung anzuzeigen und anzupassen.

MELDUNGSFENSTER UND POP-UP-MELDUNGEN

Bei der Arbeit von Kaspersky Security treten unterschiedliche Ereignisse ein. Die Ereignisse können informativen Charakter besitzen oder wichtige Informationen enthalten. Ein Ereignis kann beispielsweise über die erfolgreiche Aktualisierung des Programms informieren oder auf einen Fehler während der Virensuche oder der Ausführung von Datei-Anti-Virus und Web-Anti-Virus hinweisen, der dringend behoben werden muss.

Das Programm informiert Sie über das Eintreten von Ereignissen mithilfe von *Meldungsfenstern* und *Pop-up-Meldungen*, die mit Signaltönen ergänzt werden können.

Kaspersky Security unterstützt das Benachrichtigungssystem Growl. Wenn das System Growl aktiviert ist, werden Pop-up-Meldungen mit seiner Hilfe angezeigt.

IN DIESEM ABSCHNITT

Über Meldungsfenster 26

Über Ereignistypen 26

Über Pop-up-Meldungen 26

Zustellung von Meldungen deaktivieren 26

ÜBER MELDUNGSFENSTER

Kaspersky Security zeigt Meldungsfenster auf dem Bildschirm an, wenn unterschiedliche Reaktionen auf ein Ereignis zur Auswahl stehen. Wenn das Programm beispielsweise ein schädliches Objekt findet, werden Ihnen folgende Aktionen angeboten: Objekt löschen oder Objekt desinfizieren. Das Meldungsfenster wird erst dann geschlossen, wenn Sie eine der vorgeschlagenen Aktionen auswählen.

ÜBER EREIGNISTYPEN

In Abhängigkeit davon, welche Relevanz ein Ereignis für die Computersicherheit besitzt, informiert Kaspersky Security über folgende Ereignistypen:

- **Kritische** – Meldungen über kritische Ereignisse weisen auf Probleme bei der Ausführung von Kaspersky Security oder auf Schwachstellen im Schutz Ihres Computers hin. Der Empfang von Meldungen über diese Ereignisse sollte aktiviert werden.
- **Wichtige** – Ereignisse, die unbedingt beachtet werden müssen, da sie wichtige Situationen bei der Arbeit von Kaspersky Security betreffen.
- **Informative** – Ereignisse informativen Charakters.

ÜBER POP-UP-MELDUNGEN

Kaspersky Security zeigt *Pop-up-Meldungen* an, um Sie über Ereignisse zu informieren, die keine sofortige Aktion erfordern. Pop-up-Meldungen erscheinen unter dem Programmsymbol in der Menüleiste und verschwinden bald darauf automatisch vom Bildschirm.

ZUSTELLUNG VON MELDUNGEN DEAKTIVIEREN

Kaspersky Security benachrichtigt Sie mithilfe verschiedener Methoden standardmäßig über alle Ereignisse, die mit der Ausführung des Programms zusammenhängen (s. Abschnitt "Meldungsfenster und Pop-up-Meldungen" auf Seite 25). Sie können die Zustellung von Meldungen deaktivieren oder die Ereignistypen auswählen, über die Sie benachrichtigt werden möchten. Außerdem kann der Begleitton für Meldungen ausgeschaltet werden.

Informationen über Ereignisse, die in Kaspersky Security auftreten, werden unabhängig davon, ob die Zustellung von Meldungen aktiviert oder deaktiviert ist, im Programmbericht protokolliert.

- *Gehen Sie folgendermaßen vor, um das Senden von Meldungen zu deaktivieren:*

  1. Öffnen Sie das Programmkonfigurationsfenster (siehe Seite 23), und wählen Sie die Registerkarte **Ansicht** aus.

  2. Im Block **Meldungen** können Sie das Kontrollkästchen **Meldungen zeigen** deaktivieren, um keine Benachrichtigungen in Form von Meldungsfenstern mehr zu erhalten.

- *Gehen Sie folgendermaßen vor, um die Ereignistypen auszuwählen, über die Sie benachrichtigt werden möchten:*

  1. Öffnen Sie das Programmkonfigurationsfenster (siehe Seite 23), und wählen Sie die Registerkarte **Ansicht** aus.

  2. Im Block **Meldungen** deaktivieren Sie die Kontrollkästchen der Ereignistypen (s. Abschnitt "Über Ereignistypen" auf Seite 26), über die Sie nicht mehr benachrichtigt werden möchten.

- *Um den Signalton beim Erscheinen von Meldungsfenstern und Pop-up-Meldungen zu deaktivieren, gehen Sie folgendermaßen vor:*

  1. Öffnen Sie das Programmkonfigurationsfenster (siehe Seite 23), und wählen Sie die Registerkarte **Ansicht** aus.

  2. Im Block **Meldungen** deaktivieren Sie das Kontrollkästchen neben **Signalton für Benachrichtigungen aktivieren**.

NEWS AGENT

Durch News Agent werden Sie von Kaspersky Lab über alle wichtigen Ereignisse informiert, die mit Kaspersky Security und mit dem Schutz vor Computerbedrohungen zusammenhängen.

Das Programm benachrichtigt Sie über ein Symbol im oberen Bereich des Programmhauptfensters über alle Neuigkeiten (s. Abschnitt "Programmhauptfenster" auf Seite 20).

LIZENZIERUNG DES PROGRAMMS

Dieser Abschnitt informiert über die wichtigsten Begriffe, die mit der Programmaktivierung zusammenhängen. Hier werden Lizenzvertrag, Lizenztypen, Methoden zur Programmaktivierung und Verlängerung der Lizenzgültigkeit erläutert.

IN DIESEM ABSCHNITT

Über den Lizenzvertrag 28

Über die Lizenz 28

Über den Aktivierungscode 29

Lizenz-Info anzeigen 29

Lizenz erwerben 30

Lizenz verlängern 31

Aktivierung von Kaspersky Security 32

ÜBER DEN LIZENZVERTRAG

Der Lizenzvertrag ist ein rechtsgültiger Vertrag zwischen Ihnen und Kaspersky Lab ZAO. Er bestimmt die Nutzungsbedingungen für das Programm.

Lesen Sie den Lizenzvertrag sorgfältig, bevor Sie beginnen, mit dem Programm zu arbeiten.

Die Bedingungen des Lizenzvertrags können Sie während der Installation des Kaspersky-Lab-Programms einsehen.

Sie akzeptieren den Lizenzvertrag, indem Sie dem Wortlaut des Lizenzvertrags bei der Programminstallation zustimmen. Falls Sie dem Lizenzvertrag nicht zustimmen, müssen Sie die Programminstallation abbrechen.

ÜBER DIE LIZENZ

Eine *Lizenz* begründet ein zeitlich begrenztes Nutzungsrecht für ein Programm, das Ihnen auf Basis eines Lizenzvertrags überlassen wird. Zur Lizenz gehört der individuelle Aktivierungscode Ihres Exemplars von Kaspersky Security.

Die Lizenz enthält die Berechtigung zur Nutzung folgender Leistungen:

- Verwendung des Programms auf einem oder mehreren Geräten.

  Die Anzahl der Geräte, auf denen Sie das Programm nutzen dürfen, wird im Lizenzvertrag genannt.

- Kontaktaufnahme mit dem Technischen Support von Kaspersky Lab

- Nutzung sonstiger Leistungen, die Ihnen von Kaspersky Lab oder den Vertriebspartnern während der Gültigkeitsdauer der Lizenz zur Verfügung gestellt werden (s. Abschnitt "Service für Benutzer" auf S. 12).

Der Umfang der verfügbaren Leistungen und die Nutzungsdauer für das Programm sind vom Typ der Lizenz abhängig, mit der das Programm aktiviert wurde.

Die folgenden Lizenztypen sind vorgesehen:

- *Testlizenz* – eine kostenlose Lizenz zum Kennenlernen des Programms.

  Eine Testlizenz hat üblicherweise nur eine kurze Gültigkeitsdauer. Nach Ablauf der Testlizenz führt Kaspersky Security keine Funktionen mehr aus. Es muss eine kommerzielle Lizenz gekauft werden, um das Programm weiter zu verwenden.

- *Kommerzielle Lizenz* – eine kostenpflichtige Lizenz, die beim Kauf des Programms zur Verfügung gestellt wird.

  Nach Ablauf der kommerziellen Lizenz funktioniert das Programm auch weiterhin, jedoch lediglich mit eingeschränktem Funktionsumfang. Sie können Ihren Computer weiterhin auf Viren und andere Sicherheitsbedrohungen untersuchen und die anderen Programmkomponenten verwenden, allerdings nur mit Datenbanken, die beim Ablauf der Lizenz bereits installiert waren. Zur weiteren Nutzung von Kaspersky Security mit all seinen Funktionen ist eine Verlängerung der kommerziellen Lizenz erforderlich.

  Es wird empfohlen, die Gültigkeitsdauer einer Lizenz spätestens dann zu verlängern, wenn die aktive Lizenz abläuft. Nur so lässt sich ein optimaler Antiviren-Schutz für Ihren Computer gewährleisten.

ÜBER DEN AKTIVIERUNGSCODE

Der *Aktivierungscode* ist ein Code, den Sie erhalten, wenn Sie eine kommerzielle Lizenz zur Nutzung von Kaspersky Security erwerben. Dieser Code ist für die Programmaktivierung erforderlich.

Der Aktivierungscode besteht aus einer einzigartigen Codefolge von lateinischen Buchstaben und Ziffern im Format xxxxx-xxxxx-xxxxx-xxxxx.

Je nachdem, auf welche Weise Sie das Programm erworben haben, haben Sie folgende Möglichkeiten, den Aktivierungscode zu erhalten:

- Wenn Sie Kaspersky Security in einer CD-Box gekauft haben, ist der Aktivierungscode in der Dokumentation oder auf der Verpackung angegeben, in der sich die Installations-CD befindet.

- Wenn Sie Kaspersky Security in einem Internet-Shop gekauft haben, erhalten Sie den Aktivierungscode per E-Mail an die Adresse, die Sie bei der Bestellung angegeben haben.

Die Gültigkeitsdauer der Lizenz beginnt ab dem Datum der Programmaktivierung. Wenn Sie eine Lizenz erworben haben, die die Nutzung von Kaspersky Security auf mehreren Geräten zulässt, beginnt die Gültigkeitsdauer der Lizenz ab dem Datum der ersten Nutzung des Aktivierungscodes.

Wenn Sie den Aktivierungscode verlegt oder nach der Programmaktivierung unbeabsichtigt gelöscht haben, müssen Sie für seine Wiederherstellung eine Anfrage an den technischen Support von Kaspersky Lab aus Ihrem Mein Kaspersky Account senden (s. Abschnitt "Technischen Support erhalten über Mein Kaspersky Account" auf S. 57).

LIZENZ-INFO ANZEIGEN

➧ *Um Informationen über die aktuelle Lizenz anzuzeigen,*

öffnen Sie das Programmhauptfenster (siehe Seite 20), und klicken Sie auf die Schaltfläche .

In diesem Fenster (siehe Abbildung unten) werden Informationen über die Lizenznummer, den Schlüsseltyp (Aktiv- oder Reserveschlüssel), den Lizenztyp (kommerzielle oder Testlizenz), die Beschränkung bezüglich der Anzahl der Computer

angegeben, an denen Sie das Programm verwenden dürfen, sowie Datum und Uhrzeit des Ablaufs der Gültigkeitsdauer der Lizenz und die Anzahl der verbleibenden Tage bis zu diesem Datum angezeigt.

Kaspersky Security: Lizenz
365
Kommerzielle Version auf 1 Computer
aktiv
Seriennummer: 13CE-00058F-15EE4A5E
Gültigkeitsdauer: March 21, 2013 2:59 AM
Reserve-Aktivierungscode
Das Programm wird automatisch mit dem Reserve-Aktivierungscode aktiviert, wenn die aktuelle Lizenz abläuft:
Aktivieren
Beispiel: 11AA1-11AAA-1AA11-1A111
Möchten Sie die Lizenz verlängern?
Wenn Sie die Lizenz für Kaspersky Security verlängern möchten, klicken Sie auf "Verlängern" und folgen Sie den Anweisungen in unserem Online-Shop.
Verlängern

Abbildung 5. Fenster Lizenz

Wenn keine Lizenz vorhanden ist, benachrichtigt Sie Kaspersky Security darüber. Wenn das Programm nicht aktiviert ist, können Sie den Vorgang zur Aktivierung starten (siehe Abschnitt "Aktivierung von Kaspersky Security" auf Seite 32). Wenn Sie eine Testlizenz haben, können Sie eine kommerzielle Lizenz erwerben (s. Abschnitt "Lizenz erwerben " auf Seite 30).

Mit der kommerziellen Lizenz können Sie zwei Schlüsseldateien hinzufügen: einen aktiven und einen Reserveschlüssel. Die aktive Schlüsseldatei ist ab dem Zeitpunkt der Programmaktivierung gültig. Die Reserveschlüsseldatei wird direkt nach Ablauf der kommerziellen Lizenz gültig, zu der die aktive Schlüsseldatei gehört. Wenn kein Reserveschlüssel hinzugefügt wurde, und die kommerzielle Lizenz, zu der die aktive Schlüsseldatei gehört, abläuft, können Sie ihre Gültigkeitsdauer verlängern (s. Abschnitt "Lizenz verlängern" auf Seite 31).

LIZENZ ERWERBEN

Falls keine Lizenz für die Nutzung von Kaspersky Security vorliegt oder das Programm über eine Testlizenz aktiviert wurde, können Sie eine kommerzielle Lizenz erwerben.

Gehen Sie folgendermaßen vor, um eine Lizenz zu erwerben:

1. Öffnen Sie das Programmhauptfenster (siehe Seite 20), und klicken Sie auf die Schaltfläche .
2. Klicken Sie im folgenden Fenster (siehe Abbildung unten) auf die Schaltfläche **Kaufen**.

Auf der geöffneten Webseite finden Sie umfassende Informationen darüber, zu welchen Bedingungen Sie im Internet-Shop von Kaspersky Lab oder bei einem autorisierten Händler eine Lizenz erwerben können. Beim Kauf über einen Internet-Shop wird nach Zahlungseingang ein Aktivierungscode für Kaspersky Security (siehe Abschnitt "Über den Aktivierungscode" auf Seite 29) an die im Bestellformular angegebene E-Mail-Adresse geschickt.

Abbildung 6. Auswahl der Methode der Programmaktivierung

LIZENZ VERLÄNGERN

Sie müssen die Gültigkeitsdauer der Lizenz für die Nutzung des Programms nach Ablauf der gültigen kommerziellen Lizenz, zu der die aktive Schlüsseldatei gehört, verlängern, wenn keine Reserveschlüsseldatei hinzugefügt wurde. Wenn keine Verlängerung stattfindet, führt Kaspersky Security alle seine Funktionen weiterhin aus, allerdings werden die Antiviren-Datenbanken nicht mehr aktualisiert.

➧ *Gehen Sie folgendermaßen vor, um die Gültigkeitsdauer einer Lizenz zu verlängern:*

1. Öffnen Sie das Programmhauptfenster (siehe Seite 20), und klicken Sie auf die Schaltfläche .
2. Klicken Sie im folgenden Fenster auf die Schaltfläche **Verlängern**.

Dadurch wird eine Webseite geöffnet, auf der Sie umfassende Informationen darüber finden, zu welchen Bedingungen Sie im Internet-Shop von Kaspersky Lab oder bei einem der Vertriebspartner die Gültigkeitsdauer der Lizenz verlängern können. Beim Verlängern der Lizenz über einen Internet-Shop wird Ihnen nach Zahlungseingang eine E-Mail an die im Bestellformular angegebene E-Mail-Adresse geschickt, die einen Aktivierungscode für Kaspersky Security enthält (siehe Abschnitt "Über den Aktivierungscode" auf Seite 29).

AKTIVIERUNG VON KASPERSKY SECURITY

Vergewissern Sie sich vor der Aktivierung von Kaspersky Security, dass Datum und Uhrzeit des Computers korrekt eingestellt sind.

Das Programm wird aktiviert, indem eine Schlüsseldatei hinzugefügt wird, mit deren Hilfe Kaspersky Security das Vorhandensein der Rechte zur Nutzung des Programms überprüft und die Nutzungsdauer ermittelt.

Wenn das Programm nicht aktiviert ist, können Sie alle Funktionen von Kaspersky Security außer dem Update nutzen. Sie können das Programm nur einmal nach der Installation updaten.

IN DIESEM ABSCHNITT

Programm mit Testlizenz aktivieren 32

Programm mithilfe des Aktivierungscodes aktivieren 33

PROGRAMM MIT TESTLIZENZ AKTIVIEREN

Die Programmaktivierung mit einer Testlizenz ist nur dann möglich, wenn diese Version von Kaspersky Security bisher noch nicht auf dem Computer installiert war.

Es wird empfohlen, diese Aktivierungsvariante auszuwählen, wenn Sie eine Testversion des Programms verwenden möchten, bevor Sie sich zum Kauf einer kommerziellen Version entscheiden. Sie erhalten einen kostenlosen Schlüssel, dessen Gültigkeitsdauer durch die Testlizenz beschränkt ist.

Bei der Programmaktivierung mit einer Testlizenz ist eine Internetverbindung erforderlich. Ist momentan keine Internetverbindung vorhanden, so kann das Programm später mit einer Testlizenz aktiviert werden.

Gehen Sie folgendermaßen vor, um das Programm mit einer Testlizenz zu aktivieren:

1. Öffnen Sie das Programmhauptfenster (siehe Seite 20), und klicken Sie auf die Schaltfläche .
2. Klicken Sie im folgenden Fenster auf die Schaltfläche **Testlizenz**.
3. Im Fenster **Aktivierung einer Testversion des Programms** klicken Sie auf die Schaltfläche **Testversion aktivieren**.
4. Warten Sie, bis Kaspersky Security eine Verbindung mit den Servern von Kaspersky Lab hergestellt und die Daten für die Überprüfung weitergeleitet hat. Bei erfolgreicher Überprüfung erhält und installiert das Programm eine Schlüsseldatei mit einer Gültigkeitsdauer, die durch die Testlizenz begrenzt ist.

Wenn die Gültigkeit der Testlizenz für diese Version von Kaspersky Security abgelaufen ist, erscheint eine entsprechende Meldung auf dem Bildschirm. In diesem Fall können Sie eine Lizenz erwerben (s. Abschnitt "Lizenz erwerben" auf Seite 30).

Wenn die Programmaktivierung mit Testlizenz erfolgreich abgeschlossen wurde, informiert Sie Kaspersky Security darüber und zeigt Ihnen Informationen über die Lizenznummer, den Lizenztyp (Testlizenz), die Beschränkung bezüglich der Anzahl der Computer, an denen Sie das Programm verwenden dürfen, sowie Datum und Uhrzeit des Ablaufs der Gültigkeitsdauer der Lizenz und die Anzahl der verbleibenden Tage bis zu diesem Datum an.

PROGRAMM MITHILFE DES AKTIVIERUNGSCODES AKTIVIEREN

Verwenden Sie diese Aktivierungsmethode, wenn Sie eine kommerzielle Programmversion erworben und einen Aktivierungscode erhalten haben. Auf Grundlage dieses Codes erhalten Sie die Schlüsseldatei, die einen Zugang zu den Funktionen von Kaspersky Security für die Geltungsdauer der Lizenz sicherstellt.

Bei Auswahl der Anwendungsaktivierung per Aktivierungscode ist eine Internetverbindung erforderlich. Ist momentan keine Internetverbindung vorhanden, kann die Aktivierung des Programms später vorgenommen werden.

Um das Programm mithilfe eines Aktivierungscodes zu aktivieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Programmhauptfenster (siehe Seite 20), und klicken Sie auf die Schaltfläche .
2. Klicken Sie im folgenden Fenster auf **Aktivieren**.
3. Geben Sie im Fenster **Programmaktivierung** den Aktivierungscode ein, den Sie beim Kauf von Kaspersky Security erhalten haben.

   Der Aktivierungscode besteht aus einer durch Bindestriche getrennten Folge von Ziffern und Buchstaben, die in vier Blöcke zu je fünf Zeichen unterteilt ist und keine Leerzeichen enthält. Beispiel: 11AA1-11AAA-1AA11-1A111. Der Aktivierungscode muss in lateinischen Buchstaben eingegeben werden.
4. Warten Sie, bis Kaspersky Security eine Verbindung mit den Servern von Kaspersky Lab hergestellt und den eingegebenen Aktivierungscode für die Überprüfung weitergeleitet hat. Bei erfolgreicher Überprüfung des Aktivierungscodes erhält das Programm die Schlüsseldatei und fügt sie hinzu.

   Abhängig vom bereitgestellten Aktivierungscode kann Kaspersky Security den Benutzer dazu auffordern, ein obligatorisches oder nicht obligatorisches Registrierungsformular auszufüllen oder sich in Mein Kaspersky Account registrieren zu lassen (s. Abschnitt "Technischen Support erhalten über Mein Kaspersky Account" auf Seite 57).

   Wenn der Aktivierungscode bei der Überprüfung nicht validiert werden kann, erscheint eine entsprechende Meldung auf dem Bildschirm. Wenden Sie sich in diesem Fall bitte an die Firma, bei der Sie Kaspersky Security gekauft haben.
5. Kaspersky Security wird Sie über den erfolgreichen Abschluss des Aktivierungsverfahrens für das Programm informieren. Sie können sich über die Lizenznummer, den Schlüsseltyp (Aktiv- oder Reserveschlüssel) und den Lizenztyp (kommerzielle Lizenz) informieren und die Beschränkung bezüglich der Anzahl der Computer, an denen Sie das Programm verwenden dürfen, sowie Datum und Uhrzeit des Ablaufs der Gültigkeitsdauer der Lizenz und die Anzahl der verbleibenden Tage bis zu diesem Datum ansehen.
6. Klicken Sie auf die Schaltfläche **Fertig**, um zum Programmhauptfenster zurückzukehren (auf Seite 20).

PROGRAMM STARTEN UND BEENDEN

Dieser Abschnitt informiert darüber, wie das Programm gestartet und beendet wird.

Sofort nach der Installation wird das Programm automatisch gestartet und das Symbol Kaspersky Security (auf Seite 19) erscheint in der Menüleiste.

- *Um Kaspersky Security zu beenden,*

  klicken Sie auf das Symbol von Kaspersky Security (auf Seite 19) in der Menüleiste und wählen Sie im Kontextmenü den Punkt **Beenden**.

Das Programm wird beendet, und der Prozess wird aus dem Arbeitsspeicher des Computers entfernt.

Wenn Kaspersky Security beendet wird, ist Ihr Computer ungeschützt. Es besteht ein Infektionsrisiko und Ihre persönlichen Daten sind bedroht.

SCHUTZSTATUS DES COMPUTERS

Dieser Abschnitt informiert darüber, wie Bedrohungen für die Computersicherheit erkannt werden und wie die Sicherheitsstufe angepasst wird. Hier finden Sie außerdem Informationen darüber, wie der Schutz während der Arbeit des Programms aktiviert und deaktiviert werden kann.

Der Schutzstatus Ihres Computers informiert anschaulich darüber, ob momentan Bedrohungen vorhanden sind, die das allgemeine Sicherheitsniveau des Betriebssystems beeinflussen. Als Bedrohungen gelten in diesem Fall nicht nur gefundene schädliche Programme, sondern auch die Verwendung von veralteten Antiviren-Datenbanken und das Deaktivieren von Datei-Anti-Virus oder Web-Anti-Virus.

Das Schutz-Center (auf Seite 37) unterstützt Sie dabei, vorhandene Bedrohungen zu prüfen und anschließend zu beseitigen.

IN DIESEM ABSCHNITT

Schutzstatus des Computers einschätzen 35

Computerschutz deaktivieren 36

Computerschutz fortsetzen 37

Schutz-Center. 37

SCHUTZSTATUS DES COMPUTERS EINSCHÄTZEN

Der Statusindikator für den Computerschutz, der sich im rechten Bereich des Programmhauptfensters befindet, signalisiert das Auftreten von Problemen im Computerschutz (s. Abschnitt "Programmhauptfenster" auf S. 20). Die Farbe des Indikators ist vom Schutzstatus des Computers abhängig. Wenn Sicherheitsbedrohungen vorhanden sind, wird der Indikator durch einen Infotext ergänzt.

Der Schutzstatus kann durch eine der folgenden Farben signalisiert werden:

- **Grün**: Der Schutz Ihres Computers wird auf dem erforderlichen Niveau gewährleistet.

  Dies bedeutet, dass die Antiviren-Datenbanken rechtzeitig aktualisiert wurden, dass alle Schutzkomponenten mit den von Kaspersky Lab empfohlenen Einstellungen arbeiten, und dass bei der Ausführung von Untersuchungsaufgaben keine schädlichen Objekte gefunden oder die gefundenen schädlichen Objekte neutralisiert wurden. Die Kindersicherung funktioniert im normalen Modus.

- **Gelb**: Das Sicherheitsniveau Ihres Computers liegt unter dem Niveau des zuvor beschriebenen Status.

  Dieser Schutzstatus weist darauf hin, dass bei der Ausführung von Kaspersky Security Probleme vorliegen. Dieser Status tritt beispielsweise ein, wenn geringfügige Abweichungen vom empfohlenen Funktionsmodus bestehen oder die Antiviren-Datenbanken des Programms seit mehreren Tagen nicht mehr aktualisiert wurden.

- **Rot**: Für Ihren Computer besteht ein Infektionsrisiko.

  Dieser Status signalisiert, dass Probleme vorliegen, die zu einer Infektion Ihres Computers und zu Datenverlust führen können. Mögliche Probleme: Bestimmte Schutzkomponenten wurden deaktiviert, oder in einer oder mehreren Schutzkomponenten sind Störungen aufgetreten. Mögliche Probleme: Das Programm wurde schon sehr lange nicht mehr aktualisiert, das Programm wurde nicht aktiviert, oder es wurden schädliche Objekte gefunden, die dringend neutralisiert werden müssen.

Probleme und Sicherheitsrisiken sollten umgehend behoben werden. Durch einen Klick auf den Statusindikator für den Computerschutz im Programmhauptfenster öffnet sich das Fenster Schutz-Center (auf Seite 37), das detaillierte

Informationen über den Schutzstatus des Computers sowie Vorschläge für Aktionen zur Behebung von Problemen und Sicherheitsbedrohungen enthält. Die Probleme, die im Computerschutz vorliegen, sind nach Kategorien angeordnet. Für jedes Problem werden Aktionen genannt, die Sie zur Problemlösung ausführen können.

COMPUTERSCHUTZ DEAKTIVIEREN

Kaspersky Security wird in der Grundeinstellung automatisch beim Start des Betriebssystems gestartet und schützt Ihren Computer während der gesamten Sitzung. Alle Schutzkomponenten (Datei-Anti-Virus, Web-Anti-Virus) sind aktiviert und funktionieren.

Sie können den von Kaspersky Security gewährten Schutz teilweise oder komplett ausschalten.

Kaspersky Lab empfiehlt ausdrücklich, den Echtzeitschutz, der von Datei-Anti-Virus und Datei-Anti-Virus gewährleistet wird, nicht zu deaktivieren, da dies zu einer Infektion Ihres Computers und zu Datenverlust führen kann.

Folgende Merkmale informieren darüber, dass der Computerschutz deaktiviert wurde:

- deaktiviertes Programmsymbol (s. Abschnitt "Symbol von Kaspersky Security" auf Seite 19) in der Menüleiste;
- roter Statusindikator für den Computerschutz im rechten Bereich des Programmhauptfensters.

Der Computerschutz wird im Rahmen der Ausführung von Datei-Anti-Virus und Web-Anti-Virus betrachtet. Das Deaktivieren oder Anhalten dieser Schutzkomponenten übt keinen Einfluss auf die Ausführung von Aufgaben zur Virensuche und der Updateaufgabe aus.

Es gibt mehrere Methoden, um den Computerschutz vollständig auszuschalten. Die Schutzkomponenten können im Programmkonfigurationsfenster auf der Registerkarte **Schutz** deaktiviert werden.

Gehen Sie folgendermaßen vor, um den Computerschutz zu deaktivieren:

- Klicken Sie auf das Symbol von Kaspersky Security (auf Seite 19) in der Menüleiste und wählen Sie im Kontextmenü den Punkt **Schutz deaktivieren**.
- Öffnen Sie das Programmkonfigurationsfenster (auf Seite 23), wählen Sie die Registerkarte **Schutz** aus und deaktivieren Sie im Block **Allgemein** das Kontrollkästchen neben **Schutz aktivieren**.

Wenn Sie den Computerschutz deaktiviert haben, wird der Schutz nach einem Neustart von Kaspersky Security nicht automatisch gestartet. Der Computerschutz muss manuell aktiviert werden (s. Abschnitt "Computerschutz fortsetzen" auf Seite 37).

Gehen Sie folgendermaßen vor, um eine Schutzkomponente zu deaktivieren:

1. Öffnen das Programmkonfigurationsfenster (siehe Seite 23).
2. Deaktivieren Sie auf der Registerkarte **Schutz** im Block **<Komponentenname>** das Kontrollkästchen neben **<Komponentenname> aktivieren**.

Wenn Sie eine Schutzkomponente deaktiviert haben, wird sie nach einem Neustart von Kaspersky Security nicht automatisch aktiviert. Die Schutzkomponente muss manuell deaktiviert werden (s. Abschnitt "Computerschutz fortsetzen" auf Seite 37).

COMPUTERSCHUTZ FORTSETZEN

Wenn der Computerschutz oder eine Schutzkomponente (Datei-Anti-Virus oder Web-Anti-Virus) deaktiviert wurden, können der Computerschutz oder die Schutzkomponenten nur manuell auf Befehl des Benutzers fortgesetzt werden. Der Computerschutz oder die Schutzkomponenten werden nach einem Neustart von Kaspersky Security nicht automatisch aktiviert.

Gehen Sie folgendermaßen vor, um den Computerschutz zu aktivieren:

- Klicken Sie auf das Symbol von Kaspersky Security (auf Seite 19) in der Menüleiste und wählen Sie im Kontextmenü den Punkt **Schutz aktivieren**.
- Öffnen Sie das Programmkonfigurationsfenster (auf Seite 23), wählen Sie die Registerkarte **Schutz** aus und aktivieren Sie im Block **Allgemein** das Kontrollkästchen neben **Schutz aktivieren**.

Gehen Sie folgendermaßen vor, um eine Schutzkomponente zu aktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster (auf Seite 23).
2. Aktivieren Sie auf der Registerkarte **Schutz** im Block **<Komponentenname>** das Kontrollkästchen neben **<Komponentenname> aktivieren**.

Sie können auch das Schutz-Center verwenden, um den Computerschutz oder die Schutzkomponenten zu aktivieren (s. Abschnitt "Schutz-Center" auf Seite 37). Wenn der Computerschutz deaktiviert wird oder Schutzkomponenten deaktiviert werden, erhöht sich das Risiko einer Infektion des Computers erheblich. Deshalb wird eine solche Bedrohung sofort vom Schutz-Center registriert.

SCHUTZ-CENTER.

Das *Schutz-Center* unterstützt Sie dabei, vorhandene Probleme und Sicherheitsbedrohungen zu prüfen und anschließend zu beseitigen.

Um das Schutz-Center zu öffnen,

klicken Sie auf den Statusindikator für den Computerschutz im Programmhauptfenster (s. Abschnitt "Programmhauptfenster" auf Seite 20).

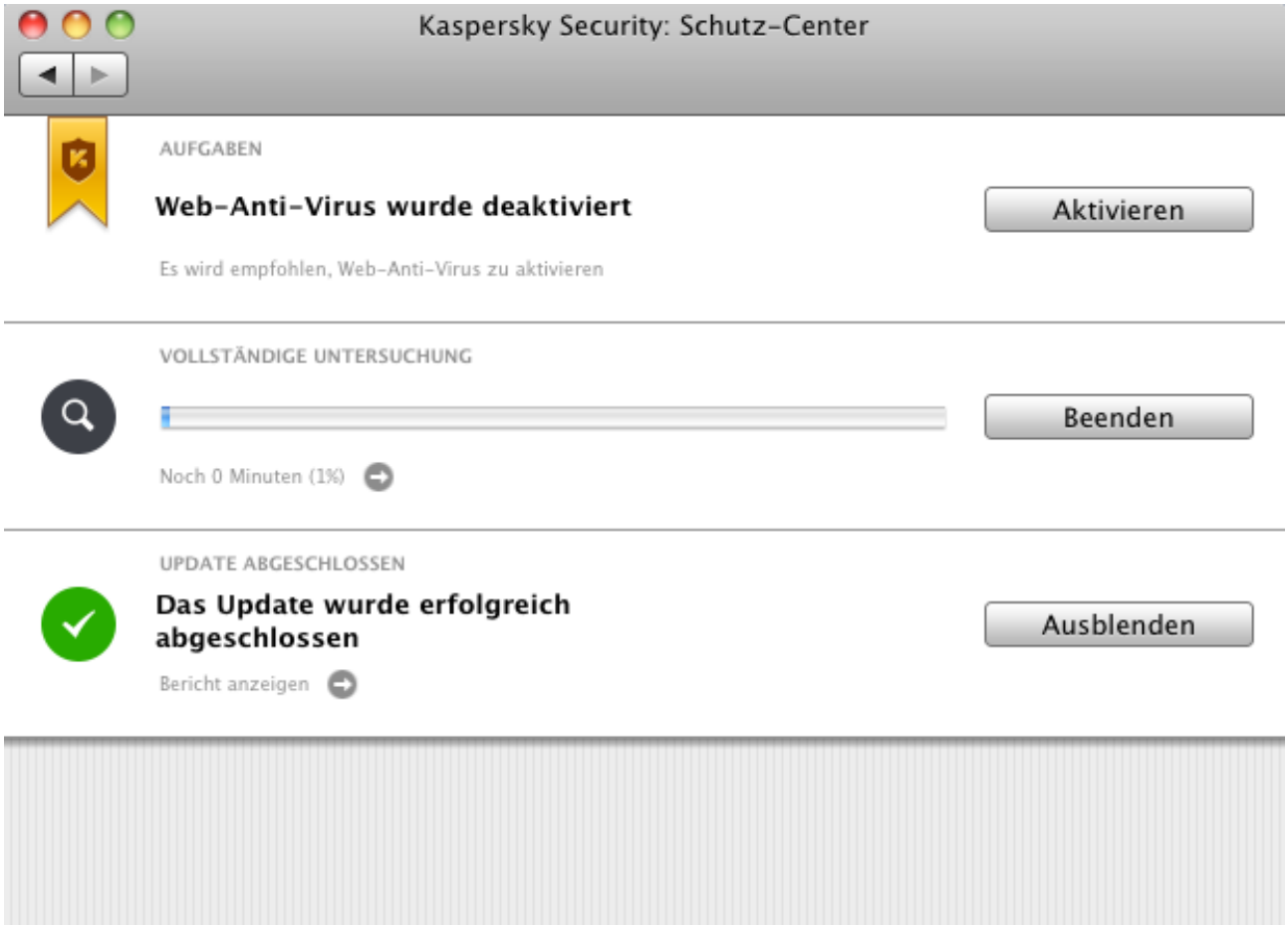


Abbildung 7. Fenster Schutz-Center

Im Fenster des Schutz-Centers (siehe Abbildung oben) können Sie eine Liste der vorhandenen Probleme und Sicherheitsbedrohungen ansehen. Probleme und Sicherheitsbedrohungen sind nach Kategorien angeordnet. Für die einzelnen Probleme und Bedrohungen werden Aktionen genannt, die dazu dienen, ein Problem zu lösen oder eine Bedrohung zu neutralisieren. Folgende Aktionen werden vorgeschlagen:

- Sofort beheben.

  Zur Beseitigung der Bedrohung, klicken Sie auf die Schaltfläche mit der Angabe der empfohlenen Aktion. Wenn beispielsweise auf Ihrem Computer infizierte Objekte erkannt worden sind, wird die Aktion **Desinfizieren** vorgeschlagen. Wenn die Antiviren-Datenbanken veraltet sind, wird die Aktion **Aktualisieren** vorgeschlagen.

- Behebung aufschieben.

  Wenn Sie eine Bedrohung nicht sofort beseitigen möchten, können Sie die Neutralisierung aufschieben und die Meldung über diese Bedrohung aus der Liste ausblenden. Verwenden Sie dazu die Schaltfläche **Ausblenden**.

  Diese Möglichkeit ist für ernste Bedrohungen nicht vorgesehen. Dazu zählen beispielsweise: Vorhandensein von unbearbeiteten schädlichen Objekten, Störungen in der Funktion der Schutzkomponenten, beschädigte Dateien in den Datenbanken von Kaspersky Security.

Wenn Sie das Schutz-Center beendet haben, bevor ernsthafte Bedrohungen neutralisiert wurden, weist die Farbe des Statusindikators für den Computerschutz im Programmhauptfenster weiter auf diese Bedrohungen hin.

Darüber hinaus finden Sie im Fenster des Schutz-Centers Informationen über die Update- oder Virensuche-Aufgaben, die aktuell ausgeführt werden, und können diese Aufgaben bei Bedarf anhalten oder neu starten.

LÖSUNGEN FÜR TYPISCHE AUFGABEN

Dieser Abschnitt enthält schrittweise Anleitungen für die Ausführung wichtiger Benutzeraufgaben, die vom Programm gestartet werden.

IN DIESEM ABSCHNITT

Wie eine vollständige Virenuntersuchung des Computers ausgeführt wird 39

Computer schnell untersuchen 40

Dateien, Ordner und Laufwerke auf Viren untersuchen 40

Lizenz kaufen 40

Lizenz verlängern 41

Wie man die Datenbanken und Programm-Module aktualisiert 41

Schutz der Daten vor einem Abfangen über die Tastatur 41

Beschränken der Nutzungsdauer des Internets 42

Einschränken des Besuchs von Websites und des Downloads von Dateien aus dem Internet 43

Einschränken von Kontakten und Korrespondenzen des Benutzers in sozialen Netzwerken 43

Schutz persönlicher Daten vor dem Versand über soziale Netzwerke 44

Empfohlene Aktionen bei blockiertem Zugriff auf eine Datei 44

Was tun, wenn Sie vermuten, dass ein Objekt von einem Virus infiziert ist? 45

Wie ein Objekt wiederhergestellt wird, das vom Programm gelöscht oder desinfiziert wurde 46

Bericht über die Programmaktivität anzeigen 46

Empfohlene Aktionen beim Erscheinen von Meldungsfenstern und Pop-up-Meldungen 47

WIE EINE VOLLSTÄNDIGE VIRENUNTERSUCHUNG DES COMPUTERS AUSGEFÜHRT WIRD

Zum Programm Kaspersky Security gehört eine Standardaufgabe zur vollständigen Untersuchung des Computers. Bei der Ausführung dieser Aufgabe untersucht das Programm alle Festplattenlaufwerke des Computers auf Viren und andere Sicherheitsbedrohungen.

Um die Aufgabe zur vollständigen Untersuchung des Computers zu starten, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Programmhauptfenster (siehe Seite 20), und klicken Sie auf die Schaltfläche .

2. Wählen Sie im folgenden Menü die Task **Vollständige Suche** aus.

Das Ergebnis der Ausführung des Tasks wird im Berichtsfenster angezeigt.

COMPUTER SCHNELL UNTERSUCHEN

Zum Programm Kaspersky Security gehört eine Standardaufgabe zur schnellen Untersuchung des Computers. Wenn diese Funktion ausgeführt wird, untersucht das Programm kritische Bereiche des Computers auf Viren und andere Sicherheitsbedrohungen: Ordner, die Dateien des Betriebssystems enthalten, und Systembibliotheken, deren Beschädigung durch schädliche Programme zur Störung des Betriebssystems Ihres Computers führen kann.

- *Um die Aufgabe zur schnellen Untersuchung des Computers zu starten, gehen Sie folgendermaßen vor:*

1. Öffnen Sie das Programmhauptfenster (siehe Seite 20), und klicken Sie auf die Schaltfläche .
2. Wählen Sie im folgenden Menü die Aufgabe **Schnelle Suche** aus.

Das Ergebnis der Ausführung des Tasks wird im Berichtsfenster angezeigt.

DATEIEN, ORDNER UND LAUFWERKE AUF VIREN UNTERSUCHEN

Wenn ein einzelnes Objekt (eine der Festplatten, ein einzelner Ordner, eine Datei, oder ein Wechseldatenträger) auf Viren oder andere Sicherheitsbedrohungen geprüft werden soll, verwenden Sie die integrierte Aufgabe zur Virensuche.

- *Um ein einzelnes Objekt auf Viren und andere Sicherheitsbedrohungen zu untersuchen, gehen Sie folgendermaßen vor:*

1. Öffnen Sie das Programmhauptfenster (siehe Seite 20), und klicken Sie auf die Schaltfläche .
2. Wählen Sie im folgenden Menü die Task **Virensuche** aus.

   Daraufhin wird das Fenster zur Auswahl von Untersuchungsobjekten geöffnet.
3. Erstellen Sie eine Liste der zu untersuchenden Objekte.

   Die Untersuchungsaufgabe wird automatisch gestartet.

Das Ergebnis der Ausführung des Tasks wird im Berichtsfenster angezeigt.

LIZENZ KAUFEN

Wenn Sie Kaspersky Security installiert haben und keine Lizenz besitzen, können Sie eine kommerzielle Lizenz nach der Programminstallation erwerben. Beim Kauf einer Lizenz erhalten Sie einen Aktivierungscode, mit dem das Programm aktiviert wird (s. Abschnitt "Kaspersky Security aktivieren" auf Seite 32).

- *Gehen Sie folgendermaßen vor, um eine Lizenz zu erwerben:*

1. Öffnen Sie das Programmhauptfenster (siehe Seite 20), und klicken Sie auf die Schaltfläche .
2. Klicken Sie im folgenden Fenster auf die Schaltfläche **Kaufen**.

Die Webseite des Internet-Shops von Kaspersky Lab wird geöffnet. Dort können Sie eine Lizenz erwerben.

LIZENZ VERLÄNGERN

Wenn die kommerzielle Lizenz, mit der Kaspersky Security aktiviert wurde, bald abläuft, können Sie diese verlängern. Nach der Verlängerung einer Lizenz erhalten Sie einen Aktivierungscode, mit dem Sie das Programm aktivieren können (siehe Abschnitt "Kaspersky Security aktivieren" auf Seite 32).

Gehen Sie folgendermaßen vor, um die Gültigkeitsdauer einer Lizenz zu verlängern:

1. Öffnen Sie das Programmhauptfenster (siehe Seite 20), und klicken Sie auf die Schaltfläche .
2. Klicken Sie im folgenden Fenster auf die Schaltfläche **Verlängern**.

   Die Webseite des Internet-Shops von Kaspersky Lab wird geöffnet. Dort können Sie die Lizenz verlängern.

WIE MAN DIE DATENBANKEN UND PROGRAMM-MODULE AKTUALISIERT

Kaspersky Lab aktualisiert die Datenbanken und Programm-Module von Kaspersky Security und veröffentlicht die Updates auf speziellen Updateservern. *Kaspersky-Lab-Updateserver* sind Internetseiten von Kaspersky Lab, auf denen Updates für Kaspersky Security regelmäßig zur Verfügung gestellt werden.

Um die Updates von den Servern herunterzuladen, ist eine Verbindung Ihres Computers mit dem Internet erforderlich.

Kaspersky Security überprüft in der Grundeinstellung regelmäßig, ob auf den Kaspersky-Lab-Servern neue Updates vorhanden sind. Wenn der Server neue Updates enthält, werden sie von Kaspersky Security im Hintergrund heruntergeladen und auf Ihrem Computer installiert.

Um Kaspersky Security zu aktualisieren,

öffnen Sie das Programmhauptfenster (siehe Seite 20), und klicken Sie auf die Schaltfläche .

Das Ergebnis der Ausführung von Update-Tasks wird im Berichtsfenster angezeigt.

SCHUTZ DER DATEN VOR EINEM ABFANGEN ÜBER DIE TASTATUR

Bei der Arbeit im Internet ist es immer wieder notwendig, persönliche Daten, Benutzernamen und Kennwörter einzugeben. Beispiele sind die Anmeldung auf Websites, der Besuch von Internet-Shops und die Verwendung von Online-Banking.

Dabei besteht die Gefahr, dass persönliche Informationen mithilfe von Keyloggern abgefangen werden.

Mit der Virtuellen Tastatur kann das Abfangen von über die Tastatur eingegebenen Daten verhindert werden.

Die Virtuelle Tastatur kann Ihre persönlichen Daten nicht schützen, wenn eine Website gehackt wurde und die Eingabe solcher Daten fordert. In diesem Fall geraten die Informationen dem Angreifer direkt in die Hände.

Die virtuelle Tastatur schützt nur bei der Arbeit mit den Browsern Safari, Firefox™ und Google Chrome™ vor dem Abfangen persönlicher Daten.

Die virtuelle Tastatur verfügt über folgende Besonderheiten:

- Die Betätigung der Tasten der virtuellen Tastatur erfolgt durch Mausklick.
- Im Vergleich zu einer echten Tastatur ist es auf der virtuellen Tastatur nicht möglich, mehrere Tasten gleichzeitig zu drücken. Um ein Symbol einzugeben, das auf der echten Tastatur mithilfe einer Kombination mit den Tasten ALT und (oder) SHIFT eingegeben wird, muss zunächst die erste Taste (z.B. ALT) und danach die Taste mit dem gewünschten Symbol gedrückt werden.
- Die Eingabesprache wird auf der virtuellen Tastatur mithilfe der Taste in der linken unteren Ecke umgeschaltet. Durch einen Klick auf diese Taste können Sie in der Dropdown-Liste die gewünschte Eingabesprache auswählen.

Standardmäßig wird die virtuelle Tastatur automatisch auf dem Bildschirm eingeblendet, wenn im Browserfenster das Feld zur Kennworteingabe ausgewählt wurde.

Um die virtuelle Tastatur zu öffnen,

klicken Sie in der Symbolleiste in der Menüleiste des Browsers.

BESCHRÄNKEN DER NUTZUNGSDAUER DES INTERNETS

Die Zahl der Kinder und Jugendlichen, die Zugang zu Computern und zum Internet besitzen, nimmt kontinuierlich zu. Zu lange Arbeitszeiten am Computer können der Gesundheit von Kindern und Jugendlichen schaden. Wenn Sie die Nutzungsdauer des Internets für einen Benutzer einschränken möchten, können Sie dies über die Kategorie Zeitkontrolle der Komponente Kindersicherung tun.

Gehen Sie folgendermaßen vor, um die Arbeitsdauer im Internet zu beschränken:

1. Öffnen Sie Konfigurationsfenster der Kindersicherung (auf Seite 24).
2. Wählen Sie im linken Bereich des Fensters das Benutzerkonto, für das Sie die Dauer des Internetzugangs beschränken möchten.
3. Wählen Sie im rechten Fensterbereich auf der Registerkarte **Einstellungen** die Kategorie der **Benutzeraktion Zeitkontrolle** aus. Wenn die Zeitkontrolle deaktiviert ist, muss sie aktiviert werden.
4. Im Block **Beschränkung des Internetzugangs pro Tag** aktivieren Sie das Kontrollkästchen neben **Internetzugang gestatten für**.
5. Stellen Sie über den Schieberegler die gewünschte Stundenanzahl pro Tag ein und legen Sie damit fest, wie lange das Internet verwendet werden darf.
6. Im Block **Beschränkung des Internetzugangs nach Zeitplan** aktivieren Sie das Kontrollkästchen neben **Beschränkung des Internetzugangs auf bestimmte Wochentage**.
7. Geben Sie die zeitlichen Einschränkungen der Internetnutzung an Werktagen und am Wochenende an.

Den **Bericht** über die Zugriffsversuche des Benutzers auf das Internet zu erlaubten und verbotenen Zeiten können Sie über die Registerkarte Berichte ansehen.

EINSCHRÄNKEN DES BESUCHS VON WEBSITES UND DES DOWNLOADS VON DATEIEN AUS DEM INTERNET

Die Zahl der Kinder und Jugendlichen, die Zugang zu Computern und zum Internet besitzen, nimmt kontinuierlich zu. Zur Gewährleistung der Sicherheit können Sie folgende Benutzeraktivitäten beschränken:

- Besuch von Webseiten, die Zeitverlust (Chats, Online-Spiele) oder Geldverlust (Internet-Shops, Auktionen) verursachen können.
- Zugriff auf Webressourcen, die für Erwachsene bestimmt sind (z.B. Seiten, die pornografische oder extremistische Materialien enthalten, die Themen wie Waffen, Drogen und Gewalt betreffen).
- Download von infizierten Dateien.

Verwenden Sie dazu die Kategorie Web-Kontrolle der Komponente Kindersicherung.

Gehen Sie folgendermaßen vor, um den Besuch von Websites sowie den Download von Dateien aus dem Internet zu beschränken:

1. Öffnen Sie das Konfigurationsfenster der Kindersicherung (auf Seite 24).
2. Wählen Sie im linken Bereich des Fensters das Benutzerkonto aus, für das Sie den Zugriff auf Websites beschränken möchten.
3. Wählen Sie im rechten Fensterbereich auf der Registerkarte **Einstellungen** die Kategorie der Benutzeraktion **Web-Kontrolle** aus. Wenn die Web-Kontrolle deaktiviert ist, muss sie aktiviert werden.
4. Aktivieren Sie das Kontrollkästchen neben **Web-Kontrolle** und die Kontrollkästchen neben den Kategorien von Websites, den Zugang zu denen Sie sperren möchten.
5. Aktivieren Sie das Kontrollkästchen neben **Kontrolle über heruntergeladene Dateien** und die Kontrollkästchen neben den Kategorien von Dateien, deren Download erlaubt ist.

Bei Bedarf können Sie den Zugriff auf einzelne Websites erlauben, die der Kategorie der gesperrten Websites zugeordnet wurden, oder den Zugriff auf bestimmte Websites sperren, indem Sie eine Ausnahmenliste anlegen.

Auf der Registerkarte Berichte können Sie den **Bericht** über Zugriffsversuche auf blockierte Websites und den Download von verbotenen Dateikategorien anzeigen lassen.

EINSCHRÄNKEN VON KONTAKTEN UND KOMMUNIKATION DES BENUTZERS IN SOZIALEN NETZWERKEN

Die Zahl der Kinder und Jugendlichen, die Zugang zu Computern und zum Internet besitzen, nimmt kontinuierlich zu. Mithilfe der Kontrolle der Kontakte und der Kommunikation von Kindern und Jugendlichen in sozialen Netzwerken können Sie verhindern, dass Fremde, die sich für Jugendliche ausgeben, Kontakt mit den Kindern aufnehmen und Zugriff auf persönliche Daten des Benutzers erhalten. Sie können die Kontakte und die Kommunikation des Benutzers in sozialen Netzwerken über die Kategorie Soziale Netzwerke der Komponente Kindersicherung einschränken.

Gehen Sie folgendermaßen vor, um Konversationen zu beschränken, die über soziale Netzwerke erfolgen:

1. Öffnen Sie das Konfigurationsfenster der Kindersicherung (auf Seite 24).
2. Wählen Sie im linken Bereich des Fensters das Benutzerkonto, für das Sie die Kommunikation in sozialen Netzwerken beschränken möchten.

3. Wählen Sie im rechten Fensterbereich auf der Registerkarte **Einstellungen** die Kategorie der Benutzeraktion **Soziale Netzwerke** aus. Wenn die Kontrolle über soziale Netzwerke deaktiviert ist, muss sie aktiviert werden.

4. Legen Sie eine Liste mit erlaubten und verbotenen Kontakten an. Klicken Sie dazu auf die Schaltfläche und geben Sie im Feld der Spalte **Identifikator** den Namen des Kontakts im sozialen Netzwerk (Login) und im Feld der Spalte **Name** den echten Namen des Kontakts ein. Standardmäßig ist die Kommunikation mit dem Kontakt aus der Liste verboten.

5. Wenn Sie die Kommunikation mit einem Kontakt temporär erlauben möchten, wählen Sie diesen Kontakt aus der Liste und deaktivieren Sie das Kontrollkästchen in der Spalte **Gesperrt**. Die Kommunikation mit diesem Kontakt wird so lange erlaubt, bis das Kontrollkästchen wieder aktiviert wird.

Wenn die Kommunikation mit einem Kontakt verboten ist, werden alle Nachrichten, die sich an diesen Kontakt richten oder von ihm stammen, blockiert.

Auf der Registerkarte **Berichte** können Sie folgende Informationen sehen:

- Informationen über Nachrichten, die vom gesperrten Kontakt erhalten oder an ihn adressiert wurden;
- Informationen über das Vorhandensein von persönlichen Daten in den Nachrichten;
- Text der Kommunikation mit jedem Kontakt.

SCHUTZ PERSÖNLICHER DATEN VOR DEM VERSAND ÜBER SOZIALE NETZWERKE

Kaspersky Security erlaubt es, die mit der Arbeit am Computer und im Internet verbundenen Risiken zu reduzieren. Sie können anhand der Kategorie Persönliche Daten der Komponente Kindersicherung verbieten, dass Daten, die persönliche Informationen enthalten, über soziale Netzwerke und bei Datenübertragungen über Websites verschickt werden.

Gehen Sie folgendermaßen vor, um das Senden von persönlichen Daten zu verbieten:

1. Öffnen Sie das Konfigurationsfenster der Kindersicherung (auf Seite 24).

2. Wählen Sie im linken Bereich des Fensters das Benutzerkonto, für das Sie den Versand persönlicher Daten verbieten möchten.

3. Wählen Sie im rechten Fensterbereich auf der Registerkarte **Einstellungen** die Aktionskategorie **Persönliche Daten**. Wenn die Kontrolle über persönliche Daten deaktiviert ist, muss sie aktiviert werden.

4. Liste mit persönlichen Daten anlegen. Klicken Sie dazu auf die Schaltfläche und geben Sie die Daten im Feld der Spalten **Beschreibung** und **Daten** ein. Sie können beispielsweise Einträge für die Kreditkartennummer, die Postanschrift oder die Telefonnummer anlegen. Standardmäßig ist das Senden von Daten, die der Liste hinzugefügt wurden, verboten.

Kaspersky Security blockiert alle Versuche des Sendens von Daten, die der Liste hinzugefügt wurden. Auf der Registerkarte **Berichte** sehen Sie Informationen über blockierte Nachrichten.

EMPFOHLENE AKTIONEN BEI BLOCKIERTEM ZUGRIFF AUF EINE DATEI

Kaspersky Security blockiert den Zugang zur Datei oder zum Programm, wenn Datei-Anti-Virus vermutet, dass das angefragte Objekt mit einem schädlichen Programm infiziert oder möglicherweise infiziert ist.

- *Um erkannte gefährliche Objekte zu bearbeiten, gehen Sie folgendermaßen vor:*

1. Öffnen Sie das Programmhauptfenster (siehe Seite 20), und klicken Sie auf die Schaltfläche .

   Daraufhin wird das Berichtsfenster von Kaspersky Security geöffnet.

2. Wählen Sie im linken Bereich des Berichtsfensters **Erkannte Bedrohungen** aus.

   Im rechten Bereich des Fensters der Gruppe **Aktiv** wird eine Liste mit gefundenen gefährlichen Objekten mit Statusangabe angezeigt. Durch einen Klick auf das Symbol erweitern Sie die Liste der Objekte.

3. Klicken Sie auf die Schaltfläche **Alle desinfizieren**. Für jedes Objekt erscheint auf dem Bildschirm eine Meldung, in dem Sie über das weitere Vorgehen mit dem Objekt entscheiden können. Wenn Sie im Meldungsfenster das Kontrollkästchen **In allen ähnlichen Fällen anwenden** aktivieren, wird die ausgewählte Aktion auf alle Objekte mit dem gleichen Status angewendet.

- *Um die möglicherweise infizierten Objekte zu bearbeiten, die in die Quarantäne verschoben wurden, gehen Sie folgendermaßen vor:*

1. Öffnen Sie das Programmhauptfenster (siehe Seite 20), und klicken Sie auf die Schaltfläche .

   Daraufhin wird das Berichtsfenster von Kaspersky Security geöffnet.

2. Wählen Sie im linken Bereich des Fensters **Quarantäne** aus.

   Auf der rechten Seite des Fensters wird der Inhalt des Speichers angezeigt.

3. Klicken Sie auf die Schaltfläche **Alle untersuchen**, um alle möglicherweise infizierten Quarantäne-Objekte mit den aktuellen Datenbanken von Kaspersky Security zu untersuchen.

4. Klicken Sie auf die Schaltfläche **Wiederherstellen**, um die Dateien in einem vom Benutzer vorgegebenen Ordner oder in dem Ordner, aus dem sie in die Quarantäne verschoben wurden (standardmäßig), wiederherzustellen.

   Es wird empfohlen, nur Objekte mit dem Status *Fehlalarm* wiederherzustellen, da die Wiederherstellung anderer Objekte zu einer Infektion Ihres Computers führen kann.

5. Klicken Sie auf die Schaltfläche **Löschen** oder **Alle löschen**, um das ausgewählte Objekt aus der Quarantäne zu löschen oder um die Quarantäne vollständig zu löschen.

Wenn Sie überzeugt sind, dass Objekte, die von Datei-Anti-Virus gesperrt wurden, sicher sind, können Sie diese Objekte zur vertrauenswürdigen Zone hinzufügen.

WAS TUN, WENN SIE VERMUTEN, DASS EIN OBJEKT VON EINEM VIRUS INFIZIERT IST?

Wenn Sie vermuten, dass ein Objekt infiziert sein könnte, prüfen Sie es auf Viren (siehe Abschnitt "Wie eine Datei, ein Ordner oder ein Laufwerk auf Viren untersucht wird" auf Seite 40).

Wenn Kaspersky Security als Ergebnis der Prüfung mitteilt, dass das Objekt nicht infiziert ist, Sie aber das Gegenteil vermuten, verschieben Sie das Objekt in die *Quarantäne*. Objekte, die sich in der Quarantäne befinden, werden in eingepackter Form gespeichert und stellen keine Bedrohung für Ihren Computer dar. Möglicherweise kann die Bedrohung eindeutig bestimmt und desinfiziert werden, nachdem die Datenbanken von Kaspersky Security aktualisiert wurden.

Um ein Objekt in den Quarantäne-Speicher zu verschieben, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Programmhauptfenster (siehe Seite 20), und klicken Sie auf die Schaltfläche .

   Daraufhin wird das Berichtsfenster von Kaspersky Security geöffnet.

2. Wählen Sie im linken Bereich des Fensters **Quarantäne** aus.

   Auf der rechten Seite des Fensters wird der Inhalt des Speichers angezeigt.

3. Klicken Sie auf die Schaltfläche **Objekt hinzufügen** und wählen Sie im folgenden Standardfenster die benötigte Datei aus. Die Datei erscheint in der Liste mit dem Status *Vom Benutzer hinzugefügt*.

WIE EIN OBJEKT WIEDERHERGESTELLT WIRD, DAS VOM PROGRAMM GELÖSCHT ODER DESINFIZIERT WURDE

Es wird davor gewarnt, gelöschte und desinfizierte Objekte wiederherzustellen, falls dies nicht absolut erforderlich ist, da diese Objekte eine Gefahr für Ihren Computer darstellen können.

Manchmal gelingt es bei der Desinfektion von infizierten Objekten nicht ihre Unversehrtheit zu sichern. Wenn ein desinfiziertes Objekt wichtige Informationen enthielt, die aufgrund der Desinfektion vollständig oder teilweise verloren gegangen sind, können Sie versuchen, das ursprüngliche Objekt über seine Sicherungskopie wiederherzustellen.

Gehen Sie folgendermaßen vor, um ein Objekt wiederherzustellen, das vom Programm gelöscht oder verändert wurde:

1. Öffnen Sie das Programmhauptfenster (auf Seite 20), und klicken Sie auf die Schaltfläche .

   Daraufhin wird das Berichtsfenster von Kaspersky Security geöffnet.

2. Wählen Sie im linken Bereich des Fensters **Backup** aus.

   Daraufhin wird der Inhalt des Backups in Form einer Liste mit Sicherungskopien der Objekte im rechten Bereich des Fensters angezeigt.

3. Wählen Sie die Sicherungskopie des gewünschten Objekts in der Liste aus, und klicken Sie auf die Schaltfläche **Wiederherstellen**. Bestätigen Sie die Aktion im folgenden Fenster. Das Objekt wird unter dem gleichen Namen am ursprünglichen Speicherort wiederhergestellt, den es vor der Desinfektion und Löschung trug. Wenn sich am ursprünglichen Speicherort ein Objekt mit dem gleichen Namen befindet, erfolgt eine entsprechende Warnung auf dem Bildschirm. Diese Situation kann eintreten, wenn ein Objekt wiederhergestellt wird, das vor der Desinfektion gespeichert wurde. Sie können den Speicherort des wiederherzustellenden Objekts ändern oder das Objekt umbenennen.

   Es wird empfohlen sofort nach der Wiederherstellung das Objekt auf Viren zu untersuchen. Möglicherweise gelingt es, das Objekt mit aktualisierten Datenbanken ohne Datenverlust zu desinfizieren.

BERICHT ÜBER DIE PROGRAMMAKTIVITÄT ANZEIGEN

Informationen zu Ereignissen beim Ausführen des Datei-Anti-Virus, Web-Anti-Virus, Tasks zur Virensuche und Update-Tasks werden im Berichtsfenster angezeigt.

Um das Berichtsfenster zu öffnen,

öffnen Sie das Programmhauptfenster (siehe Seite 20), und klicken Sie auf die Schaltfläche .

EMPFOHLENE AKTIONEN BEIM ERSCHEINEN VON MELDUNGSFENSTERN UND POP-UP-MELDUNGEN

Programmbenachrichtigungen (siehe Abschnitt "Meldungsfenster und Pop-up-Meldungen" auf Seite 25) in Form von Pop-up-Meldungen informieren Sie über Programmereignisse, die während der Programmausführung auftreten und Ihre Aufmerksamkeit erfordern.

Erscheint eine solche Benachrichtigung auf dem Bildschirm, muss eine der vorgegebenen Varianten für die weitere Vorgehensweise ausgewählt werden. Als optimale Aktion gilt die von Kaspersky Lab Experten standardmäßig empfohlene Variante.

BEDIENUNG DES PROGRAMMS ÜBER DIE BEFEHLSZEILE

Sie können Kaspersky Security mithilfe der Befehlszeile steuern.

Syntax der Befehlszeile:

```
kav <Befehl> [Einstellungen]
```

Als <Befehl> können Sie verwenden:

- **help** – Hilfe zur Befehlssyntax, Anzeige einer Befehlsliste.
- **scan –** Untersuchung auf das Vorhandensein schädlicher Programme.
- **update –** Programm-Update starten;
- **rollback –** Rollback des letzten durchgeführten Updates von Kaspersky Security (für die Ausführung des Befehls sind Administratorrechte erforderlich);
- **start** – Start einer Schutzkomponente oder eines Tasks;
- **stop –** Beenden einer Schutzkomponente oder Aufgabe (für die Ausführung des Befehls sind Administratorrechte erforderlich);
- **status** – Aktuellen Status einer Komponente oder Task auf dem Bildschirm anzeigen;
- **statistics**– Die Statistik über die Arbeit einer Schutzkomponente oder eines Tasks auf dem Bildschirm anzeigen;
- **export –** Export der Arbeitseinstellungen einer Schutzkomponente oder eines Tasks;
- **import –** Import der Arbeitseinstellungen einer Schutzkomponente oder Aufgabe (für die Ausführung des Befehls sind Administratorrechte erforderlich);
- **addkey –** Aktivierung des Programms mithilfe einer Schlüsseldatei (für die Ausführung des Befehls sind Administratorrechte erforderlich);
- **exit –** Beenden des Programms (für die Ausführung des Befehls sind Administratorrechte erforderlich).

Jedem Befehl entspricht eine bestimmte Auswahl von Parametern.

IN DIESEM ABSCHNITT

Hilfe anzeigen 49

Virensuche 49

Programm-Update 51

Rollback zum vorherigen Update 52

Beenden einer Komponente oder einer Aufgabe 53

Statistik über die Arbeit einer Komponente oder Aufgabe 54

Schutzparameter exportieren 54

Schutzparameter importieren 54

Programm aktivieren 55

Programm beenden 55

Rückgabecodes der Befehlszeile 55

HILFE ANZEIGEN

Zur Anzeige der Hilfe über die Syntax der Befehlszeile dient folgender Befehl:

```
kav [ -? | help ]
```

Um Hilfe über die Syntax eines konkreten Befehls zu erhalten, können Sie einen der folgenden Befehle verwenden:

```
kav <Befehl> -?
kav help <Befehl>
```

VIRENSUCHE

Eine Befehlszeile für den Start der Untersuchung eines Bereichs auf Viren sieht im Allgemeinen folgendermaßen aus:

```
kav scan [<Untersuchungsobjekt>] [<Aktion>] [<Dateitypen>] [<Ausnahmen>]
[<Berichtsparameter>] [<zusätzliche Parameter>]
```

Für die Virensuche können Sie auch die im Programm erstellten Aufgaben verwenden, indem Sie die entsprechende aus der Befehlszeile starten (siehe Abschnitt "Starten / Beenden einer Komponente oder einer Aufgabe" auf Seite 53). Die Aufgabe wird mit den Einstellungen ausgeführt, die über die Programmoberfläche von Kaspersky Security festgelegt wurden.

Beschreibung der Parameter

<Untersuchungsobjekt> – Dieser Parameter legt eine Liste der Objekte fest, die auf schädlichen Code analysiert werden sollen. Der Parameter kann mehrere Werte aus der folgenden Liste enthalten. Die Werte werden durch Leerzeichen getrennt:

<files> - Liste mit den Pfaden der Dateien und / oder Ordner für die Untersuchung. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Als Trennzeichen für die Elemente der Liste dient das Leerzeichen. Kommentare:

- wenn der Objektname oder der Pfad eine Lücke oder spezielle Symbole enthält ($, &, @ usw.), muss er durch einfache Einführungszeichen eingeschlossen werden, oder das ausgeschlossene Symbol muss auf der linken Seite durch einen Backslash getrennt werden;
- wenn ein konkreter Ordner angegeben wird, werden alle darin enthaltenen Dateien und Ordner untersucht.

-all – Vollständige Untersuchung des Computers;

-remdrives – Alle Wechseldatenträger;

-fixdrives – Alle lokalen Laufwerke;

-netdrives – Alle Netzlaufwerke;

-quarantine – Objekte, die in die Quarantäne verschoben wurden;

-@:<filelist.lst> – Pfad der Datei mit einer Liste der Objekte und Ordner, die untersucht werden sollen. Die Datei muss das Textformat besitzen. Jedes Untersuchungsobjekt muss in einer separaten Zeile stehen. Nur die Angabe des absoluten Pfads der Datei ist zulässig.

Wenn keine Liste der Objekte für die Untersuchung angegeben wurde, führt Kaspersky Security die Aufgabe Virensuche mit den Einstellungen aus, die über die Programmoberfläche festgelegt wurden.

<Aktion> – legt fest, wie während der Virenprüfung gefundene schädliche Objekte behandelt werden sollen. Wenn der Parameter nicht angegeben wird, wird standardmäßig die Aktion ausgeführt, die dem Wert **-i8** entspricht. Folgende Varianten stehen zur Auswahl:

-i0- Keine Aktion ausführen, nur Informationen im Bericht protokollieren;

-i1 – Infizierte Objekte desinfizieren; wenn die Desinfektion nicht möglich ist – überspringen;

-i2 – die infizierten Objekte desinfizieren, wenn eine Desinfektion unmöglich ist – löschen; keine Container löschen, außer den Containern mit dem Ausführungstitel (sfx-Archive);

-i3 - infizierte Objekte desinfizieren; wenn die Desinfektion nicht möglich ist – löschen; Container-Objekte vollständig löschen, wenn die darin enthaltenen infizierten Dateien nicht gelöscht werden können;

-i4 - infizierte Objekte löschen; Container-Objekte vollständig löschen, wenn die darin enthaltenen infizierten Dateien nicht gelöscht werden können;

-i8 - beim Fund eines infizierten Objekts den Benutzer nach der Aktion fragen. Diese Aktion wird standardmäßig verwendet;

-i9 - den Benutzer nach der Aktion fragen, wenn die Untersuchung abgeschlossen wird.

<Dateitypen> – Der Parameter bestimmt die Typen der Dateien, die auf Viren untersucht werden. Wenn der Parameter nicht angegeben wird, werden standardmäßig nur infizierbare Dateien nach ihrem Inhalt untersucht. Folgende Varianten stehen zur Auswahl:

-fe – Nur infizierbare Dateien nach Erweiterung untersuchen;

-fi – Nur infizierbare Dateien nach Inhalt untersuchen (standardmäßig);

-fa – Alle Dateien untersuchen.

<Ausnahmen> – legt fest, welche Objekte von der Untersuchung ausgeschlossen werden sollen. Man kann einige Parameter aus der folgenden Liste aufführen und diese in Probleme aufteilen:

-e:a – Archive nicht untersuchen;

-e:b – Mail-Datenbanken nicht untersuchen;

-e:m – E-Mail-Nachrichten im Textformat nicht untersuchen;

-e:<mask> – Objekte mit Maske nicht prüfen;

-e:<seconds> – Objekte überspringen, deren Untersuchung länger dauert, als der durch den Parameter in Sekunden angegebene Zeitraum;

-es:<size> – Objekte überspringen, deren Größe den angegebenen Wert in Megabyte übersteigt.

<Berichtsparameter> – Der Parameter bestimmt das Format des Berichts über die Untersuchungsergebnisse. Die Verwendung eines absoluten oder relativen Pfads zur Datei für eine Berichtsspeicherung ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt.

-r:<report_file> – Nur wichtige Ereignisse in der angegebenen Berichtsdatei protokollieren;

-ra:<report_file> – Alle Ereignisse in der angegebenen Berichtsdatei protokollieren.

<Erweiterte Einstellungen> – Einstellungen für die Anwendung von Virenprüfungsverfahren und der Konfigurationsdatei für Einstellungen:

-iSwift=<on|off> – Verwendung der Technologie iSwift aktivieren / deaktivieren;

-c:<Name_der Konfigurationsdatei> – bestimmt den Pfad zur Konfigurationsdatei, die die Arbeitseinstellungen des Programms bei der Ausführung der Aufgaben zur Virensuche enthält. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn kein Parameter festgelegt ist, werden neben den Werten, die bereits in der Befehlszeile angegeben sind, Werte benutzt, die auf der Programmoberfläche festgelegt sind.

Beispiel:

Eine Untersuchung der Ordner ~/Documents, /Applications und der Datei my test.exe starten:

```
kav scan ~/Documents /Applications 'my test.exe'
```

Untersuchung der Objekte, deren Liste in der Datei object2scan.txt angegeben ist. Für die Arbeit soll die Konfigurationsdatei scan_settings.txt verwendet werden. Über die Untersuchungsergebnisse soll ein Bericht erstellt werden, in dem alle Ereignisse aufgezeichnet werden:

```
kav scan -@:objects2scan.txt -c:scan_settings.txt -ra:scan.log
```

Beispiel für die Konfigurationsdatei:

```
-netdrives -@:objects2scan.txt -ra:scan.log
```

PROGRAMM-UPDATE

Der Befehl für das Update der Programm-Module und Antiviren-Datenbanken des Programms besitzt folgende Syntax:

```
avp.com UPDATE [<Updatequelle>] [/APP=<on|off>] [<Berichtsparameter>]
[<erweiterte_Einstellungen>]
```

Beschreibung der Parameter

<Updatequelle> – HTTP-, FTP-Server oder ein Netzwerk- oder Lokalordner zum Download von Updates. Wenn der Pfad nicht angegeben wird, wird die Updatequelle aus den Parametern des Diensts für das Programm-Update übernommen.

-app=<on|off> – Update der Programm-Module aktivieren / deaktivieren.

<Berichtsparameter> – Der Parameter bestimmt das Format des Berichts über die Untersuchungsergebnisse. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt. Folgende Varianten stehen zur Auswahl:

-r:<report_file> – Nur wichtige Ereignisse in der angegebenen Berichtsdatei protokollieren;

-ra:<report_file> – Alle Ereignisse in der angegebenen Berichtsdatei protokollieren.

<Erweiterte Einstellungen> – Einstellung für die Anwendung der Konfigurationsdatei für Einstellungen.

-c: <Name_der_Konfigurationsdatei> – bestimmt den Pfad der Konfigurationsdatei, in der die Parameter für die Arbeit des Programms bei der Updateausführung enthalten sind. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Werte verwendet, die über die Programmoberfläche festgelegt wurden.

Beispiel:

Die Datenbanken des Programms aus der Quelle standardmäßig aktualisieren, alle Ereignisse im Bericht aufzeichnen:

```
kav update -ra:avbases_upd.txt
```

Update der Programm-Module von Kaspersky Security, die Parameter der Konfigurationsdatei updateapp.ini verwenden:

```
kav update -app=on -c:updateapp.ini
```

ROLLBACK ZUM VORHERIGEN UPDATE

Befehlssyntax:

```
kav rollback [<Berichtsparameter>]
```

Für die Ausführung des Befehls sind Administratorrechte erforderlich.

Beschreibung der Parameter

<Berichtsparameter> – Der Parameter bestimmt das Format des Berichts über die Ergebnisse der Rollback-Funktion. Die Angabe des absoluten und relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt.

-r:<report_file> – Nur wichtige Ereignisse in der angegebenen Berichtsdatei protokollieren;

-ra:<report_file> – Alle Ereignisse in der angegebenen Berichtsdatei protokollieren.

Beispiel:

```
kav rollback -ra:rollback.txt
```

BEENDEN EINER KOMPONENTE ODER EINER AUFGABE

Syntax des start-Befehls:

```
kav start <Profil|Aufgabenname> [<Berichtsparameter>]
```

Syntax des stop-Befehls:

```
kav stop <Profil|Aufgabenname>
```

Für die Ausführung des Befehls stop sind Administratorrechte erforderlich.

Beschreibung der Parameter

<Berichtsparameter> – Der Parameter bestimmt das Format des Berichts über die Untersuchungsergebnisse. Die Angabe des absoluten und relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt. Folgende Varianten stehen zur Auswahl:

-r:<report_file> – Nur wichtige Ereignisse in der angegebenen Berichtsdatei protokollieren;

-ra:<report_file> – Alle Ereignisse in der angegebenen Berichtsdatei protokollieren. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt.

<Profil|Taskname> – Sie müssen einen der folgenden Werte eingeben:

file_monitoring (fm) – Datei-Anti-Virus;

web_monitoring (wm) – Web-Anti-Virus;

scan_my_computer (full) – Task zur vollständigen Untersuchung des Computers;

scan_objects – Untersuchung von Objekten;

scan_quarantine – Quarantäne untersuchen;

scan_critical_areas (quick) - Schnelle Untersuchung des Computers;

updater – Updatetask.

rollback – Task Rollback des Updates.

Die aus der Befehlszeile gestarteten Komponenten und Aufgaben werden mit den Parametern ausgeführt, die über die Programmoberfläche festgelegt wurden.

Beispiel:

Um Datei-Anti-Virus zu aktivieren, geben Sie in der Befehlszeile ein:

```
kav start fm
```

Um die Aufgabe zur vollständigen Untersuchung zu beenden, geben Sie in der Befehlszeile ein:

```
kav stop scan_my_computer
```

STATISTIK ÜBER DIE ARBEIT EINER KOMPONENTE ODER AUFGABE

Syntax des status-Befehls:

```
kav status [<Profil|Aufgabenname>]
```

Syntax des statistics-Befehls:

```
kav statistics <Profil|Aufgabenname>
```

Beschreibung der Parameter

<Profil|Aufgabenname> – wird einer der Werte angegeben, die für den Befehl aufgelistet sind start / stop (siehe Abschnitt "Arbeit der Komponente oder Aufgabe starten / beenden" auf Seite 53).

Wenn der Befehl status ohne eine Wertangabe für den Parameter gestartet wird **<Profil|Taskname>**, wird auf dem Bildschirm der aktuelle Status aller Tasks und Komponenten des Programms aufgezeigt. Für den Befehl statistics soll der Wert des Parameters **<Profil|Taskname>** unbedingt angegeben werden.

SCHUTZPARAMETER EXPORTIEREN

Befehlssyntax:

```
kav export <Profil|Aufgabenname> <Dateiname>
```

Beschreibung der Parameter

<Profil|Aufgabenname> – wird einer der Werte angegeben, die für den Befehl aufgelistet sind start / stop (siehe Abschnitt "Arbeit der Komponente oder Aufgabe starten / beenden" auf Seite 53).

<Datei_name> – Pfad der Exportdatei für Einstellungen. Ein absoluter oder relativer Pfad kann angegeben werden.

Beispiel:

```
kav export fm fm_settings.txt – Textformat
```

SCHUTZPARAMETER IMPORTIEREN

Befehlssyntax:

```
kav import <Dateiname>
```

Für die Ausführung des Befehls sind Administratorrechte erforderlich.

Beschreibung der Parameter

<Datei_name> – Pfad der Importdatei für Einstellungen. Ein absoluter oder relativer Pfad kann angegeben werden.

Beispiel:

```
kav import settings.dat
```

PROGRAMM AKTIVIEREN

Die Aktivierung von Kaspersky Security kann durch die Verwendung einer Schlüsseldatei ausgeführt werden.

Befehlssyntax:

```
kav addkey <Dateiname>
```

Für die Ausführung des Befehls sind Administratorrechte erforderlich.

Beschreibung der Parameter

<Dateiname> – die Schlüsseldatei zum Programm mit der Erweiterung key.

Beispiel:

```
kav addkey 1AA111A1.key
```

PROGRAMM BEENDEN

Befehlssyntax:

```
kav exit
```

Für die Ausführung des Befehls sind Administratorrechte erforderlich.

RÜCKGABECODES DER BEFEHLSZEILE

Die allgemeinen Codes können von einem beliebigen Befehl der Befehlszeile zurückgegeben werden. Zu den Rückgabecodes für Aufgaben zählen die allgemeinen Codes sowie spezifische Codes für einen konkreten Aufgabentyp.

Allgemeine Rückgabecodes:

- 0 – Operation wurde erfolgreich ausgeführt.
- 1 – Ungültiger Parameterwert.
- 2 – Unbekannter Fehler.
- 3 – Fehler bei Ausgabenausführung.
- 4 – Aufgabenausführung wurde abgebrochen.

Rückgabecodes für Aufgaben zur Virensuche:

- 101 – Alle gefährlichen Objekte wurden verarbeitet.
- 102 – Es wurden gefährliche Objekte gefunden.

KONTAKTAUFNAHME MIT DEM TECHNISCHEN SUPPORT

Dieser Abschnitt beschreibt, wie Sie technische Unterstützung erhalten, und nennt die Voraussetzungen, die dafür erfüllt sein müssen.

IN DIESEM ABSCHNITT

Wie Sie technischen Kundendienst erhalten 56

Telefonischer Technischer Support 56

Technischen Support über Mein Kaspersky Account erhalten 57

Protokolldatei verwenden 58

Protokolldatei erstellen 58

WIE SIE TECHNISCHEN KUNDENDIENST ERHALTEN

Um Informationen über die Support-Möglichkeiten von Kaspersky Security zu erhalten,

öffnen Sie das Programmhauptfenster (siehe Seite 20), und klicken Sie auf die Schaltfläche .

Wenn Sie in der Programmdokumentation und in den Informationsquellen zum Programm keine Lösung für Ihr Problem finden können, empfehlen wir Ihnen, sich an den Technischen Support von Kaspersky Lab zu wenden. Die Mitarbeiter des Technischen Supports beantworten Ihre Fragen zur Installation und Verwendung des Programms.

Beachten Sie bitte die Regeln für die Nutzung des Technischen Supports, bevor Sie sich an den Technischen Support wenden (http://support.kaspersky.de/support/rules).

Eine Kontaktaufnahme mit den Support-Experten ist auf folgende Weise möglich:

- Telefonisch. Sie können sich am Telefon von den Spezialisten des lokalen oder internationalen Technischen Supports beraten lassen.
- Aus Mein Kaspersky Account auf der Webseite des Technischen Supports eine Anfrage senden. Sich können sich über ein Webformular an die Support-Experten wenden.

Der Technische Support wird nur für die Benutzer bereitgestellt, die eine kommerzielle Lizenz für die Nutzung des Programms erworben haben. Benutzern mit Testlizenzen steht der Technische Support nicht zur Verfügung.

TELEFONISCHER TECHNISCHER SUPPORT

Bei dringenden Problemen können Sie jederzeit den lokalen oder internationalen Technischen Support anrufen (http://support.kaspersky.com/de/support/international).

Bitte lesen Sie die Supportrichtlinien (http://support.kaspersky.com/de/support/details), bevor Sie sich an den Technischen Support wenden. Dadurch können Ihnen unsere Spezialisten schneller behilflich sein.

TECHNISCHEN SUPPORT ÜBER MEIN KASPERSKY ACCOUNT ERHALTEN

Mein Kaspersky Account ist Ihr persönlicher Bereich (https://my.kaspersky.com/de) auf der Seite des Technischen Supports.

Sie müssen sich auf der Login-Seite anmelden (https://my.kaspersky.com/ru/registration?LANG=de). Geben Sie Ihre E-Mail-Adresse und ein Kennwort für den Zugriff auf Ihren Kaspersky Account an.

Im Mein Kaspersky Account können Sie folgende Aktionen ausführen:

- Anfragen an den technischen Support und an das Virenlabor senden.
- ohne E-Mail mit dem Technischen Support kommunizieren.
- den Status Ihrer Anfragen in Echtzeit verfolgen
- Verlauf Ihrer Anfragen an den Technischen Support ansehen.
- Kopie einer Schlüsseldatei erhalten, falls die Schlüsseldatei verloren gegangen ist oder gelöscht wurde.

E-Mail-Anfrage an den technischen Support

Anfragen an den Technischen Support können per E-Mail auf Deutsch, Englisch, Französisch, Spanisch oder Russisch gestellt werden.

Füllen Sie folgende Felder des elektronischen Formulars aus:

- Typ der Anfrage.
- Name und Versionsnummer des Programms.
- Anfragetext.
- Kundennummer und Kennwort.
- E-Mail-Adresse.

Die Support-Spezialisten richten ihre Antwort an Mein Kaspersky Account und an die E-Mail-Adresse, die in der Anfrage angegeben wurde.

Elektronische Anfrage an das Virenlabor

Beachten Sie, dass für die Bearbeitung bestimmter Anfragen nicht der Technischen Support, sondern das Virenlabor verantwortlich ist.

Sie können folgende Anfragetypen an das Virenlabor richten:

- *Unbekanntes Schadprogramm* – Sie haben den Verdacht, dass eine Datei einen Virus enthält, obwohl Kaspersky Security sie nicht als infiziert einstuft.

  Die Experten des Virenlabors analysieren den eingeschickten Schadcode. Wird ein bisher unbekannter Virus gefunden, so wird seine Beschreibung einer Datenbank hinzugefügt, die bei der nächsten Aktualisierung der Antiviren-Programme verfügbar gemacht wird.

- *Viren-Fehlalarm* – Kaspersky Security stuft eine bestimmte Datei als infiziert ein, während Sie sicher sind, dass die Datei virenfrei ist.

- *Anfrage für die Beschreibung eines Schadprogramms* – Sie möchten die Beschreibung eines bestimmten Virus, den Kaspersky Security gefunden hat, auf Basis seines Namens erhalten.

Anfragen an das Virenlabor können Sie auf der Seite (http://support.kaspersky.ru/virlab/helpdesk.html?LANG=de) stellen. Dazu ist keine Anmeldung bei Mein Kaspersky Account notwendig. In diesem Fall ist die Angabe eines Aktivierungscodes notwendig.

PROTOKOLLDATEI VERWENDEN

Wenn Sie sich mit einem Problem an den Technischen Support wenden, bitten die Support-Experten Sie möglicherweise darum, einen Bericht über den Systemzustand zu erstellen und den Bericht an den Technischen Support zu schicken. Zusätzlich können die Support-Experten eine *Protokolldatei* anfordern. Eine Protokolldatei ermöglicht eine schrittweise Prüfung von ausgeführten Programmbefehlen. Dadurch lässt sich erkennen, auf welcher Etappe ein Fehler aufgetreten ist.

PROTOKOLLDATEI ERSTELLEN

➧ *Gehen Sie folgendermaßen vor, um eine Protokolldatei zu erstellen:*

1. Öffnen Sie das Programmkonfigurationsfenster, und wählen Sie die Registerkarte **Berichte** aus.

2. Aktivieren Sie im Block **Protokollierung** das Kontrollkästchen **Protokollierung aktivieren**.

3. Starten Sie Kaspersky Security neu, um den Protokollierungsvorgang zu starten.

Es wird empfohlen, diese Option nur unter Anleitung eines Support-Experten von Kaspersky Lab zu nutzen.

Protokolldateien können ein bedeutendes Volumen des Laufwerks einnehmen. Nach dem Beenden der Arbeit mit den Protokolldateien wird es empfohlen, ihre Erstellung zu deaktivieren, indem man das Kontrollkästchen **Protokollierung aktivieren** auf der Registerkarte **Berichte** im Programmkonfigurationsfenster deaktiviert. Starten Sie danach Kaspersky Security neu.

GLOSSAR

A

Aktive Lizenz

Lizenz, die momentan für die Arbeit des Kaspersky-Lab-Programms verwendet wird. Die Lizenz legt die Gültigkeitsdauer für den vollen Funktionsumfang sowie die Lizenzpolitik für das Programm fest. Im Programm kann nur ein Schlüssel den Status "aktiv" besitzen.

Aktiver Schlüssel

Schlüssel, der im Augenblick für die Programmausführung verwendet wird.

B

Backup

Spezieller Speicher für Sicherungskopien von Objekten, die vor einer Desinfektion oder vor dem Löschen angelegt werden.

D

Datenbank-Update

Eine Funktion von Kaspersky-Lab-Programmen, die es ermöglicht, den Schutz des Computers auf dem neuesten Stand zu halten. Während des Updates lädt das Programm die aktuellen Datenbanken und Programm-Module von den Updateservern von Kaspersky Lab auf den Computer herunter und installiert sie automatisch.

Datenbanken

Datenbanken, die Beschreibungen der Computer-Bedrohungen enthalten, die Kaspersky Lab beim Erscheinen der Datenbanken bekannt sind. Mithilfe der Einträge in den Datenbanken kann festgestellt werden, ob die Untersuchungsobjekte schädlichen Code enthalten. Die Datenbanken werden von Kaspersky-Lab-Experten angelegt und stündlich aktualisiert.

Desinfektion von Objekten

Verarbeitungsmethode für infizierte Objekte, bei der Daten vollständig oder teilweise wiederhergestellt werden. Nicht alle infizierten Objekte können desinfiziert werden.

F

Fehlalarm

Situation, in der ein virenfreies Objekt von der Kaspersky-Lab-Anwendung als infiziert eingestuft wird, weil sein Code Ähnlichkeit mit einem Virus aufweist.

H

Heuristische Analyse

Technologie zum Erkennen von Bedrohungen, deren Informationen noch nicht in den Datenbanken von Kaspersky Lab enthalten sind. Die heuristische Analyse ermöglicht es, Objekte zu finden, deren Verhalten im System dem Verhalten von Bedrohungen ähnelt. Objekte, die mithilfe der heuristischen Analyse gefunden werden, werden als möglicherweise infiziert eingestuft. Beispielsweise kann ein Objekt als möglicherweise infiziert eingestuft werden, wenn es eine Befehlsfolge enthält, die für schädliche Objekte typisch ist (Öffnen einer Datei, Schreiben in eine Datei).

I

INFIZIERTES OBJEKT

Ein Objekt mit einem Code-Abschnitt, der vollständig mit einem Code-Abschnitt einer bekannten Bedrohung übereinstimmt. Die Kaspersky-Lab-Spezialisten warnen davor, mit solchen Objekten zu arbeiten.

K

KASPERSKY-LAB-UPDATESERVER

HTTP- und FTP-Server von Kaspersky Lab, von denen das Kaspersky-Lab-Programm Updates für Datenbanken und Programm-Module erhält.

M

MÖGLICHERWEISE INFIZIERTES OBJEKT

Ein Objekt, dessen Code entweder den modifizierten Code einer bekannten Bedrohung enthält oder einen Code, der in seinem Verhalten einer Bedrohung ähnelt.

O

OBJEKT BLOCKIEREN

Der Zugriff externer Programme auf ein Objekt wird verboten. Ein blockiertes Objekt kann nicht gelesen, ausgeführt oder geändert werden.

P

PROGRAMM AKTIVIEREN

Wechsel des Programms in einen voll funktionellen Modus. Die Aktivierung wird während oder nach der Programminstallation vom Benutzer ausgeführt. Zur Aktivierung des Programms benötigt der Benutzer einen Aktivierungscode oder eine Schlüsseldatei.

Q

QUARANTÄNE

Ein Verzeichnis, in welches das Programm von Kaspersky Lab gefundene, möglicherweise infizierte Objekte verschiebt. Die Objekte in der Quarantäne werden in verschlüsselter Form gespeichert, um ihre Auswirkung auf den Computer zu unterbinden.

R

RESERVESCHLÜSSELDATEI

Schlüssel, der das Recht auf Nutzung des Programms bestätigt, jedoch im Augenblick nicht aktiviert ist.

S

SCHUTZ

Funktionsmodus des Programms, in dem Objekte im Echtzeitmodus auf schädlichen Code untersucht werden.

Das Programm fängt jeden Versuch zum Öffnen, Schreiben und Ausführen eines Objekts ab, und durchsucht das Objekt nach Bedrohungen. Virenfreie Objekte werden für den Zugriff freigegeben, infizierte oder verdächtige Objekte werden gemäß den Aufgabenparametern verarbeitet (desinfiziert, gelöscht, in die Quarantäne verschoben).

SCHUTZSTATUS

Aktueller Schutzstatus, der das Sicherheitsniveau des Computers charakterisiert.

T

TECHNOLOGIE GROWL

Universelles Warnsystem im Betriebssystem Mac OS X. Unterstützt die installierten Arten von Meldungen: Außer den Popup-Meldungen besteht die Möglichkeit zu Audio-Meldungen, SMS- oder E-Mail-Meldungen.

Das Layout von Meldungen, die mit Hilfe von Growl angezeigt werden, kann im Abschnitt Andere unter Systemeinstellungen angepasst werden, wo Growl automatisch nach dem Download eingefügt wird.

W

WIEDERHERSTELLUNG

Ein Originalobjekt wird aus der Quarantäne oder aus dem Backup entweder an den ursprünglichen Ort, an dem das Objekt gespeichert war, bevor es in die Quarantäne verschoben, desinfiziert oder gelöscht wurde, oder in einen benutzerdefinierten Ordner verschoben.

KASPERSKY LAB

Kaspersky Lab ist ein weltweit bekannter Hersteller von Systemen, die Computer vor Viren und anderer Malware, Spam, Netzwerk- und Hackerangriffen schützen.

Seit 2008 gehört Kaspersky Lab international zu den vier führenden Unternehmen im Bereich der IT-Sicherheit für Endbenutzer (Rating des "IDC Worldwide Endpoint Security Revenue by Vendor"). Nach einer Studie des Marktforschungsinstituts COMCON TGI-Russia war Kaspersky Lab 2009 in Russland der beliebteste Hersteller von Schutzsystemen für Heimanwender.

Kaspersky Lab wurde 1997 in Russland gegründet. Inzwischen ist Kaspersky Lab ein international tätiger Konzern mit Hauptsitz in Moskau und verfügt über fünf regionale Niederlassungen, die in Russland, West- und Osteuropa, im Nahen Osten, in Afrika, Nord- und Südamerika, Japan, China und anderen Ländern aktiv sind. Das Unternehmen beschäftigt über 2.000 hochspezialisierte Mitarbeiter.

Produkte. Die Produkte von Kaspersky Lab schützen sowohl Heimanwender als auch Firmennetzwerke.

Die Palette der Heimanwender-Produkte umfasst Antiviren-Anwendungen für Desktops, Laptops, Smartphones und andere mobile Geräte.

Das Unternehmen bietet Programme und Services für den Schutz von Workstations, Datei- und Webservern, Mail-Gateways und Firewalls. In Verbindung mit Administrationstools ermöglichen es diese Lösungen, netzwerkweit einen effektiven automatisierten Schutz vor Computerbedrohungen aufzubauen. Die Produkte von Kaspersky Lab sind durch namhafte Testlabore zertifiziert, mit den Programmen der meisten Softwarehersteller kompatibel und für die Arbeit mit unterschiedlichen Hardwareplattformen optimiert.

Die Virenanalysten von Kaspersky Lab sind rund um die Uhr im Einsatz. Sie finden und analysieren jeden Tag Hunderte neuer Computerbedrohungen. Mit diesem Wissen entwickeln sie Mittel, um Gefahren zu erkennen und zu desinfizieren. Diese Informationen fließen in die Datenbanken ein, auf die die Kaspersky-Programme zurückgreifen. *Die Antiviren-Datenbanken von Kaspersky Lab werden stündlich aktualisiert*, *die Anti-Spam-Datenbanken im 5-Minuten-Takt*.

Technologien. Viele Technologien, die für ein modernes Antiviren-Programm unerlässlich sind, wurden ursprünglich von Kaspersky Lab entwickelt. Es spricht für sich, dass viele Softwarehersteller den Kernel von Kaspersky Anti-Virus in ihren Produkten einsetzen. Zu ihnen zählen SafeNet (USA), Alt-N Technologies (USA), Blue Coat Systems (USA), Check Point Software Technologies (Israel), Clearswift (UK), CommuniGate Systems (USA), Critical Path (Ireland), D-Link (Taiwan), M86 Security (USA), GFI (Malta), IBM (USA), Juniper Networks (USA), LANDesk (USA), Microsoft (USA), NETASQ (France), NETGEAR (USA), Parallels (Russia), SonicWALL (USA), WatchGuard Technologies (USA), ZyXEL Communications (Taiwan). Eine Vielzahl von innovativen Technologien des Unternehmens ist durch Patente geschützt.

Auszeichnungen. Im Verlauf eines kontinuierlichen Kampfes mit Computerbedrohungen hat Kaspersky Lab Hunderte von Auszeichnungen erworben. So wurde Kaspersky Anti-Virus 2010 in einem Test des anerkannten österreichischen Antiviren-Labors AV-Comparatives mit mehreren Premium-Awards Advanced+ ausgezeichnet. Die höchste Auszeichnung stellt für Kaspersky Lab aber das Vertrauen seiner Benutzer auf der ganzen Welt dar. Die Produkte und Technologien des Unternehmens schützen mehr als 300 Millionen Anwender. Über 200.000 Firmen zählen zu den Kunden von Kaspersky Lab.

Webseite von Kaspersky Lab:	www.kaspersky.de
Viren-Enzyklopädie:	www.securelist.com/de/
Antiviren-Labor:	newvirus@kaspersky.com (nur zum Einsenden von möglicherweise infizierten Dateien, die zuvor archiviert wurden)
	http://support.kaspersky.com/virlab/helpdesk.html?LANG=de
	(für Fragen an die Virenanalysten)
Webforum von Kaspersky Lab:	www.kaspersky.de/forum

INFORMATIONEN ZUM FREMDCODE

Informationen zum Fremdcode sind in der Datei legal_notices.txt file:///Library/Application%20Support/Kaspersky%20Lab/KAV/Doc/legal_notices.txt, enthalten, die sich im Installationsordner des Programms befindet.

MARKENHINWEISE

Eingetragene Warenzeichen und Dienstleistungsmarken sind Eigentum der jeweiligen Inhaber.

Firefox – Warenzeichen von Mozilla Foundation.

Google Chrome – Warenzeichen von Google Inc.

Mac, Mac OS und Safari – eingetragene Warenzeichen von Apple Inc.

SACHREGISTER

A

Aktivierungscode 29

B

Backup 44, 46
Benachrichtigungen 47
Benutzerdefinierte Installation 15
Berichte 46

D

Datenbanken 41
Datenverwaltung
  Backup 44, 46
  Quarantäne 44, 45

I

Installation
  benutzerdefiniert 15
  Standard 14

K

Kaspersky Lab 62
Kindersicherung 42, 43, 44

L

Lizenz 28
  Erwerb 30, 40
  Informationen 29
  Verlängerung 31, 41

P

Programm aktivieren 32
  Testversion 32
Programm deinstallieren 17
Programm mithilfe
  des Aktivierungscodes aktivieren 33
Programmhauptfenster 20
Programm-Update 41

Q

Quarantäne 44, 45

S

Schutz 36, 37
Schutz-Center. 35, 37
Standardinstallation 14
Start
  Aufgaben zur Virensuche 39, 40

U

Updateaufgabe starten.....41

V

Virensuche 39, 40

W

Wiederherstellung des Objekts 46